XDef 2019

对话·交流·合作　前沿·实用·人才

第八届全国网络与信息安全防护峰会

结合指挥控制系统理念的网络威胁情报分析与实践

主讲人姓名　周 奕

主讲人单位　武汉安天信息技术有限责任公司

1

第一章 PART ONE

指挥控制系统（C2）相关概念

指挥控制

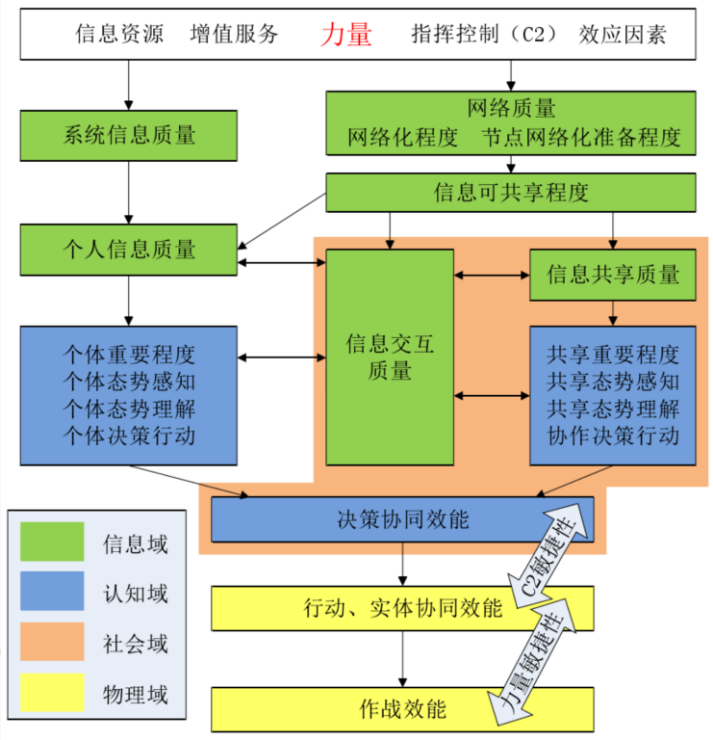
Command and Control

简称“C2”

NATO：指挥控制是合适的选定人通过形式权威和指导，利用资源分配手段，达成共同目标。

MIT：指挥员通过层级关系和组织规则依据职权和责任把所属人员组织起来

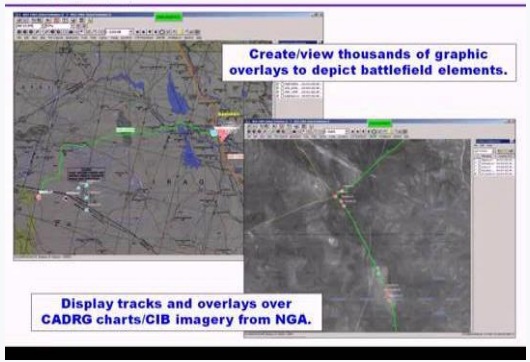
信息化战争概念框架

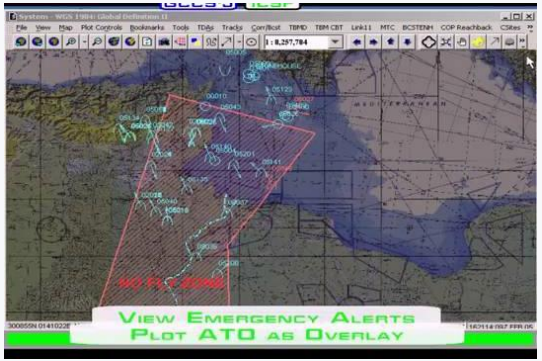


C2

- 信息获取
- 情报传输
- 态势感知
- 辅助决策
- 行动控制

指挥控制





C2

指挥强调行为的目的，控制强调行为的过程，指挥控制的核心是基于任务实现资源的优化调配和组织

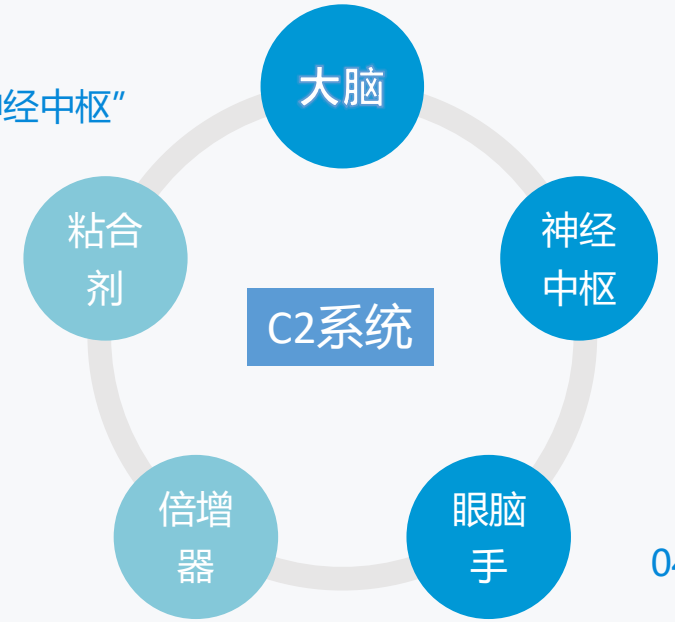
C2系统

指挥控制系统是指挥控制实现的载体，指挥控制系统运行的最终目的实现指挥控制目标

C2系统的作用

01.作战系统的“大脑”和“神经中枢”

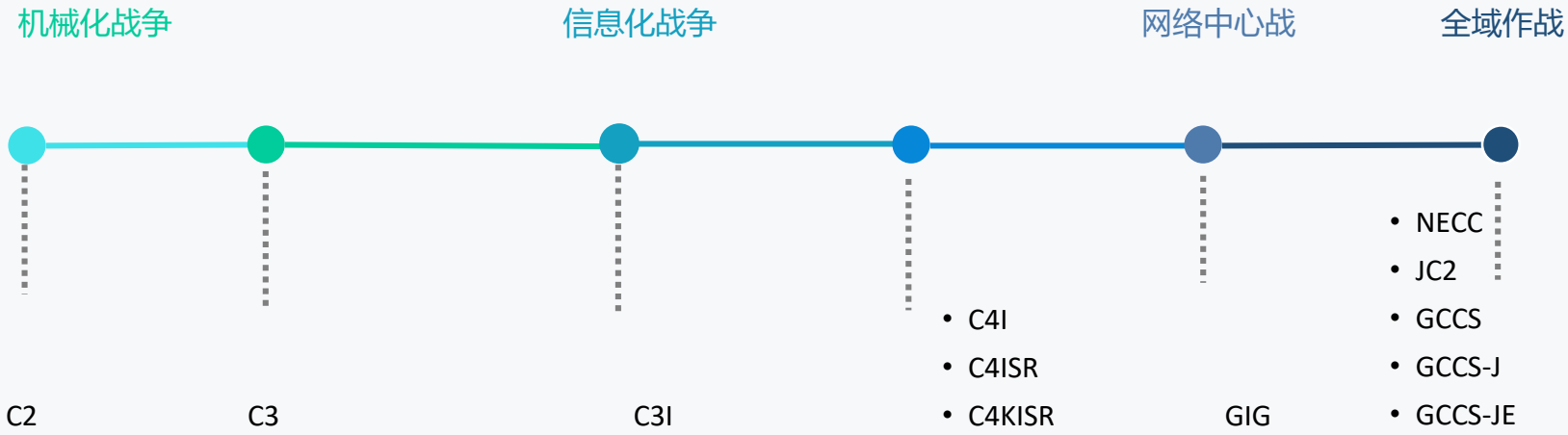
02.分散的作战单元“粘合剂”



03.作战效能“倍增器”

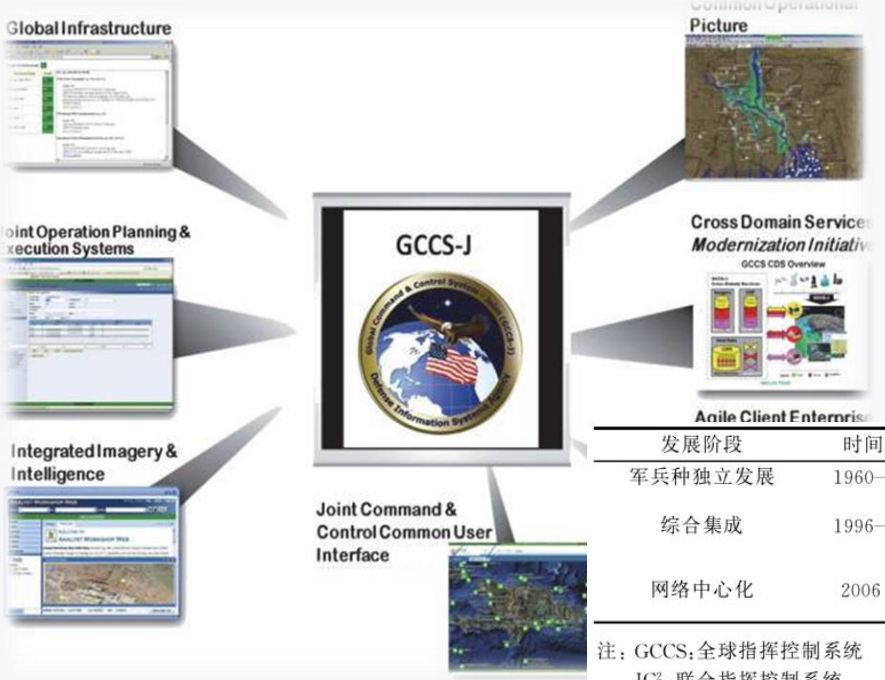
04.指挥员“眼、脑、手”延伸

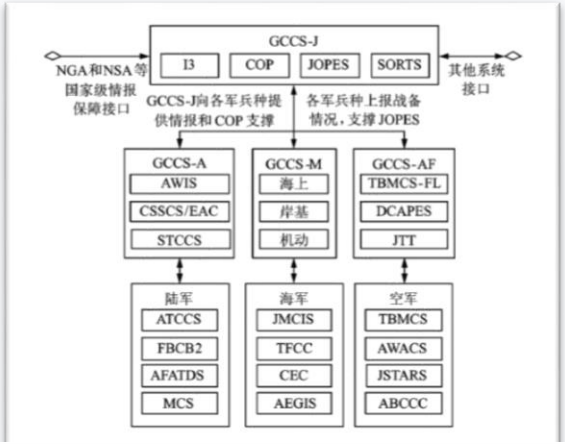
C2 系统发展历程



现代战争，由于战争空间、战争规模、战争的复杂性和不确定性、战争进程的快速性都与以往战争发生了翻天覆地的变化，对先进的指挥控制系统有着强烈的需求

C2 系统发展历程





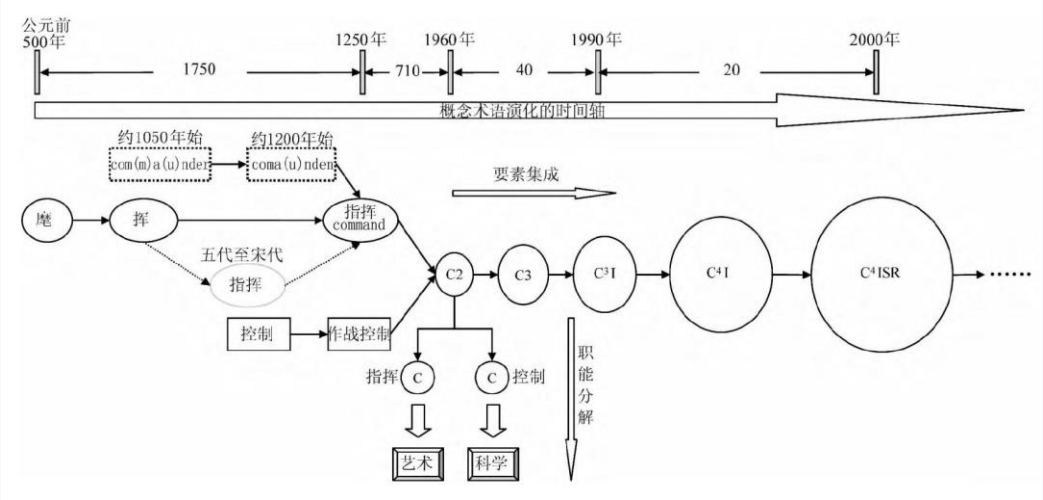
发展阶段	时间跨度	典型系统	体系结构	基础设施	技术特征
军兵种独立发展	1960—1996	WWMCCS	C/S	通信	—
综合集成	1996—2006	GCCS	段集成	国防部信息 基础设施	构件化和 综合集成技术
网络中心化	2006 至今	JC^2（NECC 和 GCCS-J Block V）	SOA	GIG	服务化和 服务集成技术

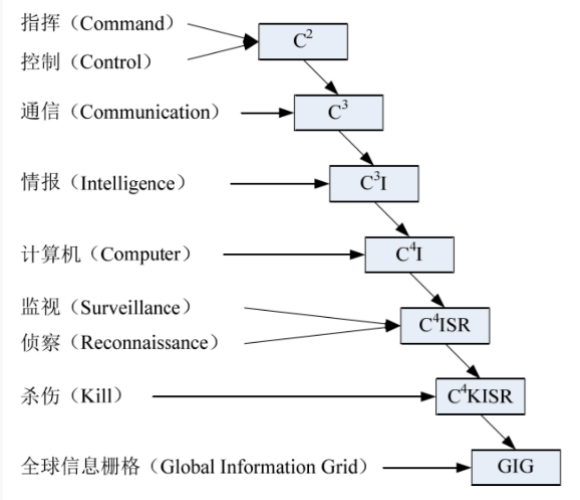
注：GCCS：全球指挥控制系统　WWMCCS：全球军事指挥控制系统　GCCS-J：联合全球指挥控制系统
JC^2：联合指挥控制系统　NECC：网络赋能指挥能力　GIG：全球信息栅格　SOA：面向服务架构

第二章 PART TWO

2 指挥控制系统发展动因及趋势分析

C2系统建设存在的问题



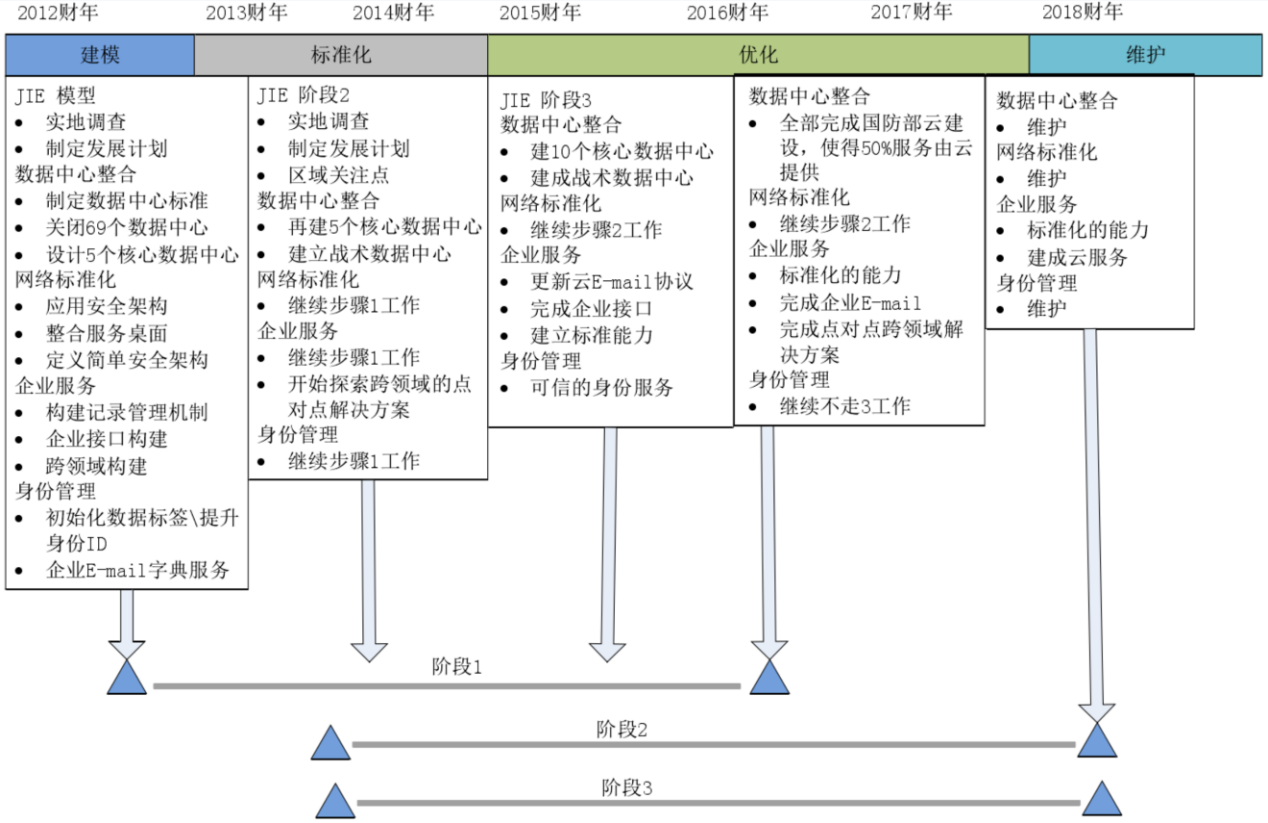


20 世纪 90 年代以来，随着信息技术的迅猛发展，原有的指挥控制系统步入爆炸式发展阶段，随着不同系统的各自发展，使得整个军事体系指挥控制系统呈现出“混乱”的发展趋势。

C2系统建设存在的问题

1	整体设计杂乱	各个部门采用不同的指挥控制系统开发语言、开发结构，不同的接口设计、O/I 设计，不同的数据格式等，使得系统间的通信以及信息共享变得十分困难
2	系统结构固化	各个指挥控制系统之间的互联关系依照既有的组织关系链接，由预先设定的组织结构确定，相对固化，重新调整部署需要更新整个系统软件，在战场环境下，无法支持指挥控制组织的敏捷调整
3	构架模式滞后	传统指挥控制观念支配下，指挥控制系统以指挥员为核心构建的，而信息化战争特点需要指挥控制系统向网络中心化、甚至是数据中心化方向转变
4	软件功能单一	大部分现有的C2系统仍停留在业务系统层面，功能较为单一，基本不具备辅助增强指挥控制敏捷性这一指挥控制系统应具备的功能，无法满足信息化战争对各层用户的要求
5	处理能力有限	信息技术的不断发展使得美军的数据获取能力得到极大提升，数据量呈现指数型增长，规模巨大、结构复杂、类型繁多、来源不同、种类各异的数据集突破了原有的有限结构化数据范畴

联合信息环境构建和发展计划



1.面向服务的系统架构

在满足安全性的基础上提供尽可能高的服务能力,更好的适应不断变化的应用需求，具有更强的敏捷性。

指挥控制系统应具备的能力

2.标准化系统环境

标准化的、单一的、安全的指挥控制系统以实现作战单元之间的安全、可靠、无缝连接

采用通用操作标准(common operational standards)实现不同网络间的资源共享

支持移动设备和轻载用户端应用

优化资源流通和共享

指挥控制系统应具备的能力

3.身份权限管理

作战资源全地域
全时域安全访问

实现数据安全和信息共享

优化身份权限管理机制

全面监控网络中用户行为
作战资源的精确化保障

实现用户的动态可控

秘密互联网协议路由网络（Secret Internet Protocol Router Network，SIPRNet）中使用“零信任（Zero-trust）”联网技术

4.应用合理化和服务虚拟化

应用合理化旨在优化为指挥控制系统提供支撑的硬件、软件以及其他相关支撑

•提高服务的灵活性，提升服务效率

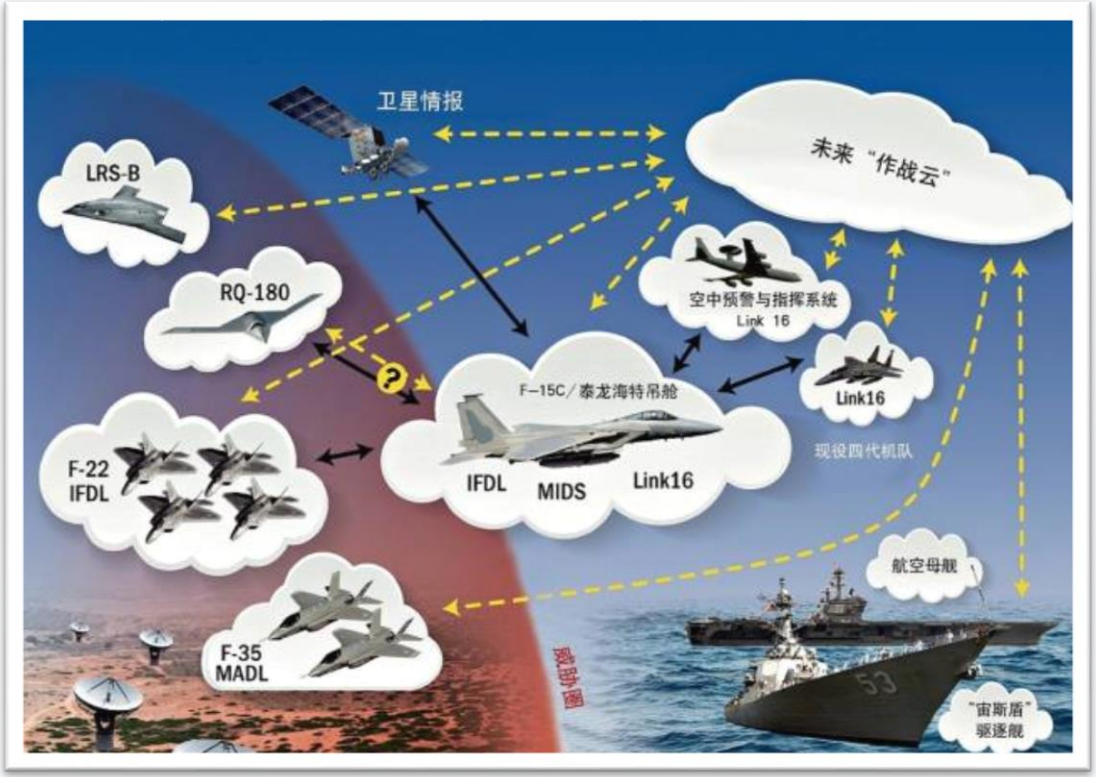
•更好的满足用户需求提高资源的利用效率

指挥控制系统应具备的能力

5.云计算

联合信息环境中，云计算模式的应用可以有效提升信息服务的灵活性和有效性，形成以云计算为核心技术体制的联合信息服务企业级应用能力

推进发展战术基础设施企业服务、战斗云、战术云等项目实践，重点解决应用服务化、云计算等技术与战术前沿适配问题

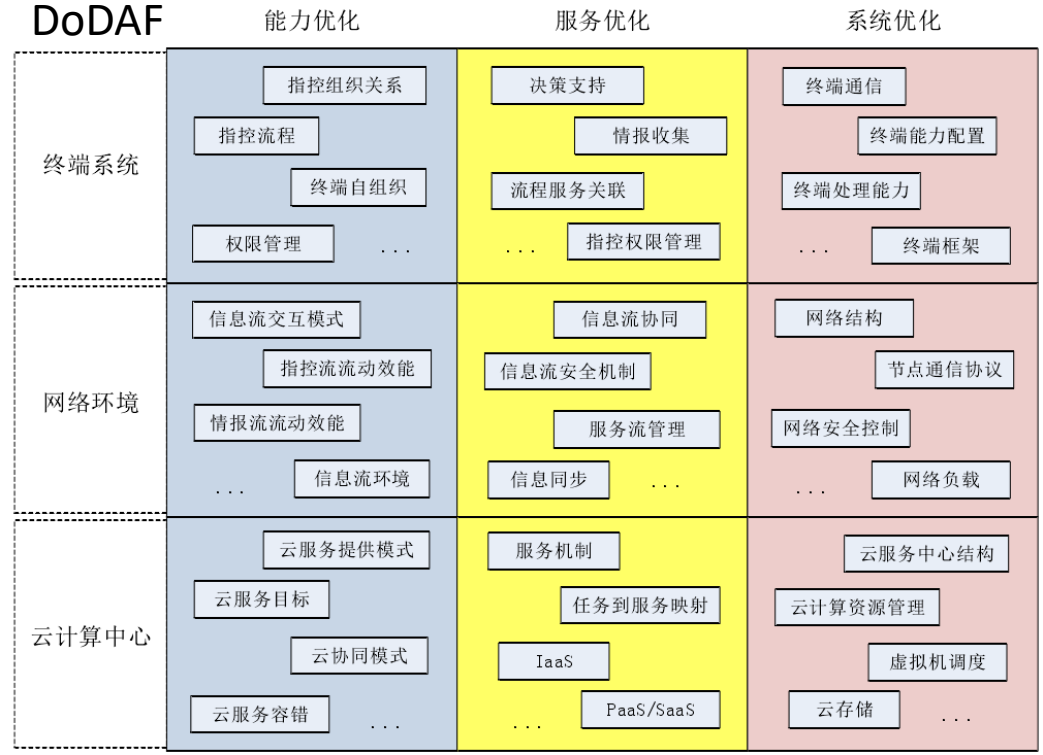


趋势分析

C2系统发展

焦点

- ✓终端系统
- ✓网络环境
- ✓信息传输
- ✓应用服务
- ✓数据安全
- ✓云计算



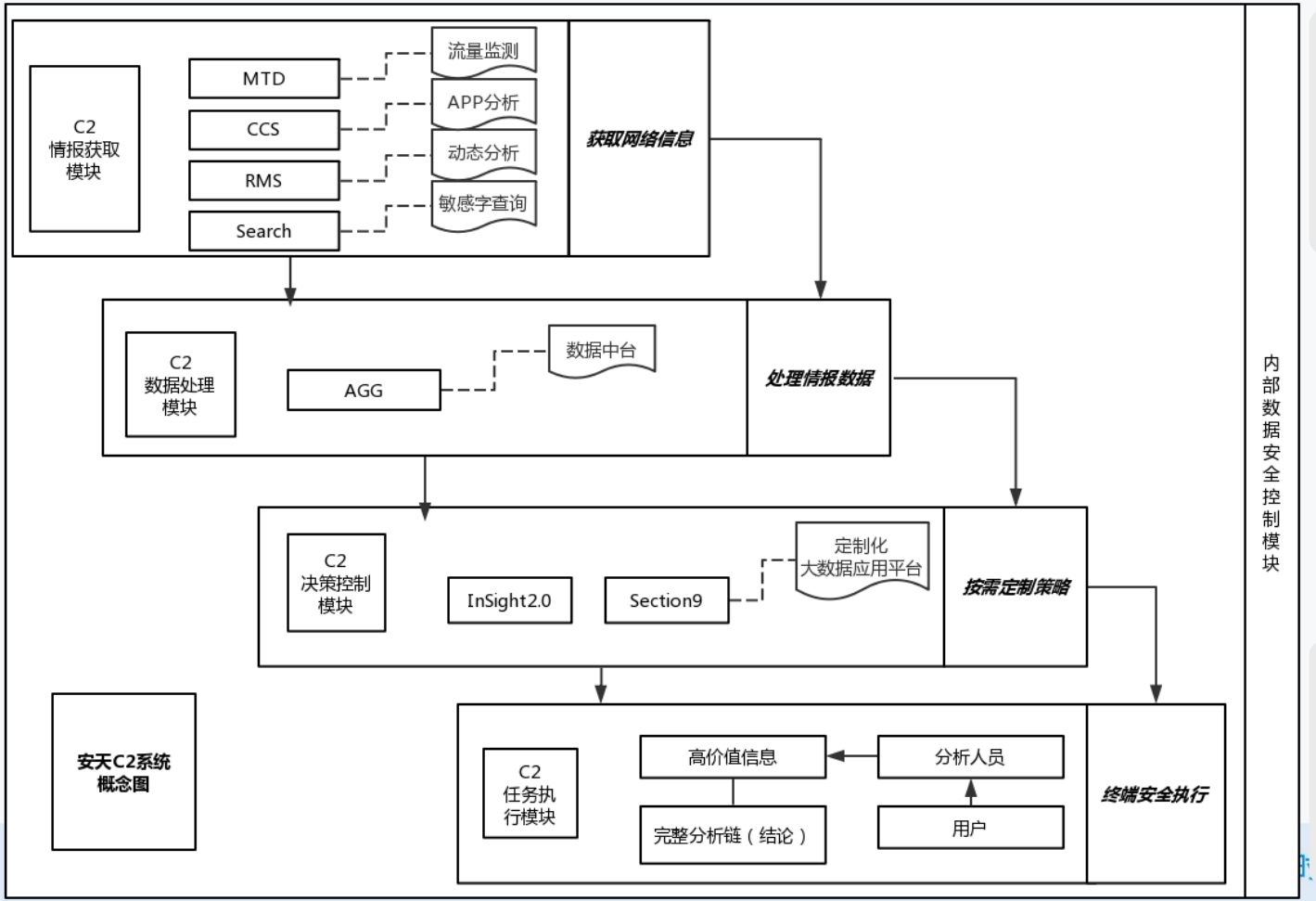
第三章 PART THREE

3

结合C2理念的网络情报分析体系设计

	基础支撑层	数据处理层	决策控制层	任务执行层	
军事C2系统	➢ 收集军事信息 • 陆/海/空/天/电/网多维探测器	➢ 处理情报数据 • 情报分析人员 • 国防情报处理系统(DI2E) • 情报信息技术系统(IC ITE)	➢ 定下作战决心 • 指挥人员 • 联合作战计划与执行系统(JOPES)	➢ 多域作战对抗 己方力量与作战对象在陆/海/空/天/电/网展开多维对抗	任务部队
安天C2系统	➢ 获取网络信息 • 客户端上报（AVL） • 情报社区收集 • 样本交换 • VDS采集	➢ 处理安全情报数据 • 大数据标准化接入（AGG模块）	➢ 按需定制策略 • 分析人员&用户 • Insight2.0(SaaS服务) • Section9 • Pos态势感知	➢ 终端安全执行 • 分析人员&用户 • 情报深挖 • 画像侧写 • 线索分析	用户

结合C2理念的网络情报分析体系设计

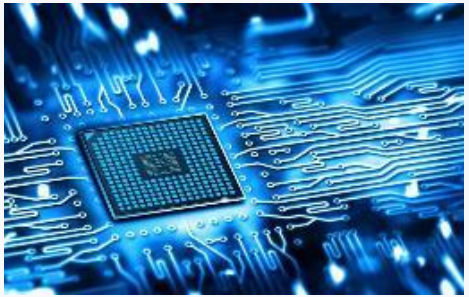


变信息为决策优势
变技术为用户服务

安天C2系统

“下游数据采集”
“上游业务应用”

1企业项目体系开发耦合用户需求



A-智能终端安全技术

战略布局、需求牵引、技术推动

服务与需求的紧耦合

B-数据处理技术

C-安全大数据技术

D-安全工具技术

E-安全服务及安全解决方案技术

2.数据规范的预处理标准化流程

01 移动终端覆盖：全球数亿

02 应用信息库：千万级+

03 终端扫描日志量：数亿/天

04 总数据量：PB级

2.数据规范的预处理标准化流程

C2系统数据模块采用先进的数据处理技术和模式，构建与具体业务松耦合的中间性的大数据处理能力，为海量多源异构数据的采集及归一化提供强大的数据抽取、转化、加载能力。

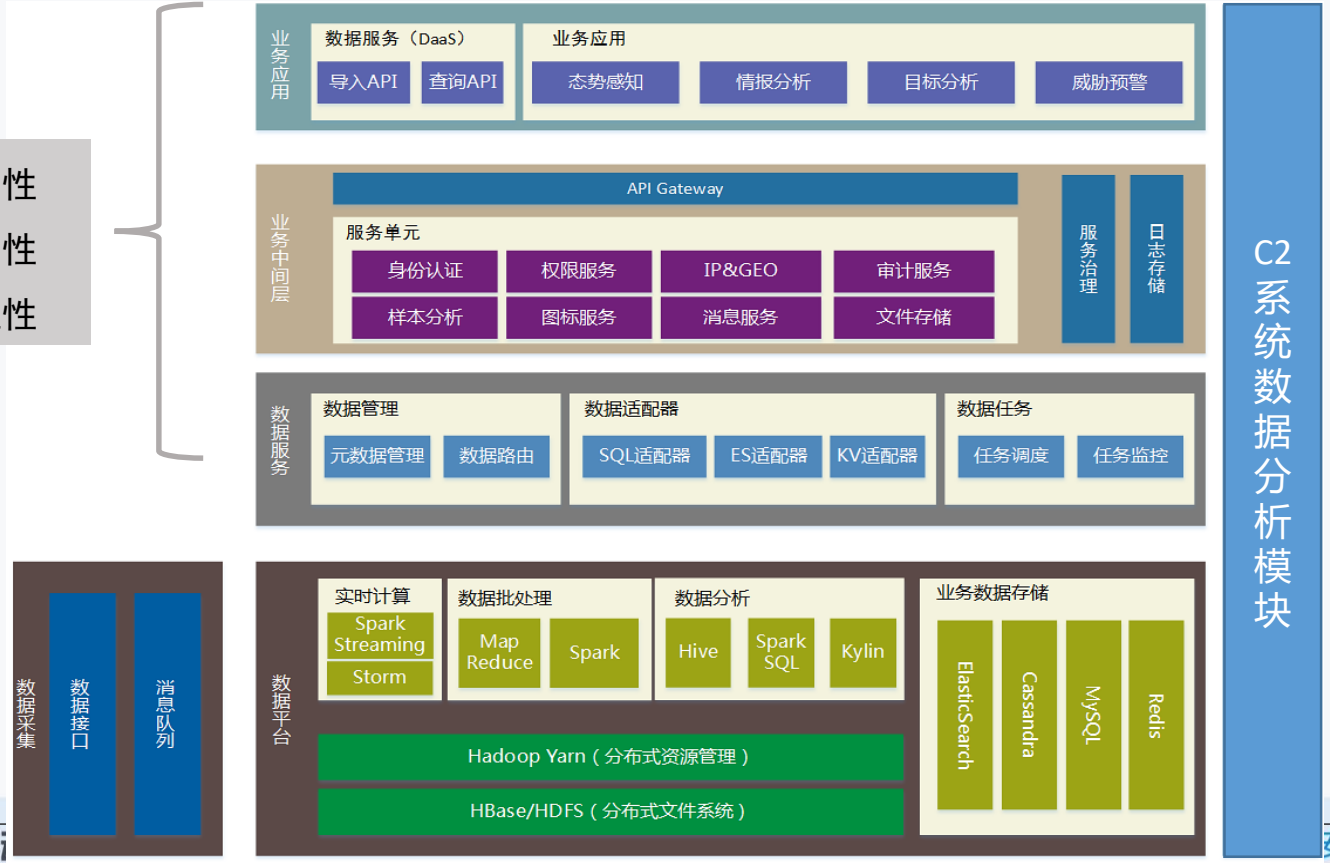
- ✓多源异构数据集成接入
- ✓分布式大数据运算处理
- ✓数据建模分析
- ✓标准对外接口
- ✓提供全链路的解决方案
- ✓强大的计算存储能力

外部数据源接入支持类型		
数据源类型	数据源分类	抽取
MySQL	关系型数据库	支持
SQL Server	关系型数据库	支持
PostgreSQL	关系型数据库	支持
Oracle	关系型数据库	支持
达梦	关系型数据库	支持
RDS for PPAS	关系型数据库	支持
HDFS	非结构化存储	支持
FTP	非结构化存储	支持
HBase	NoSQL	支持
MongoDB	NoSQL	支持
Redis	NoSQL	支持

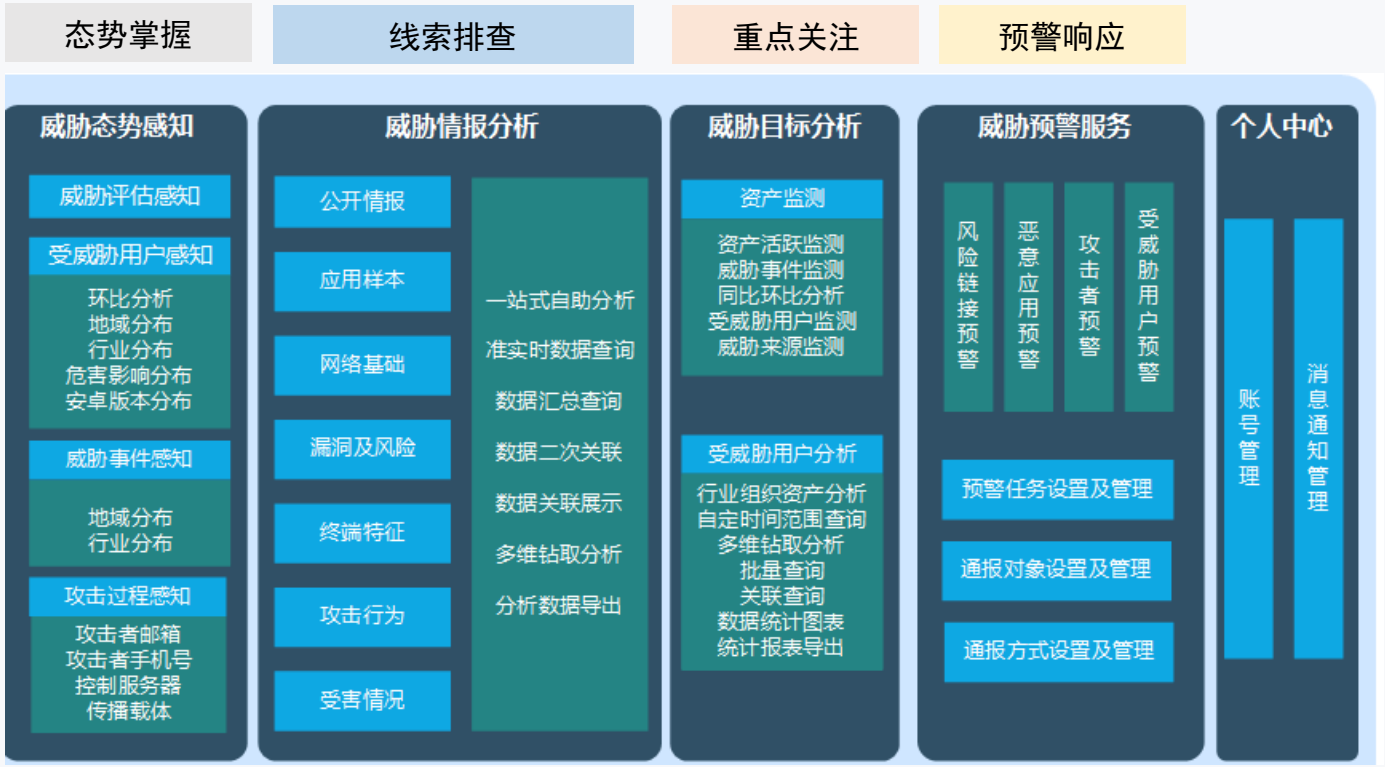
数据清洗　数据集成　数据转换　数据规约　数据存储

3. 面向服务的大数据分析模块设计

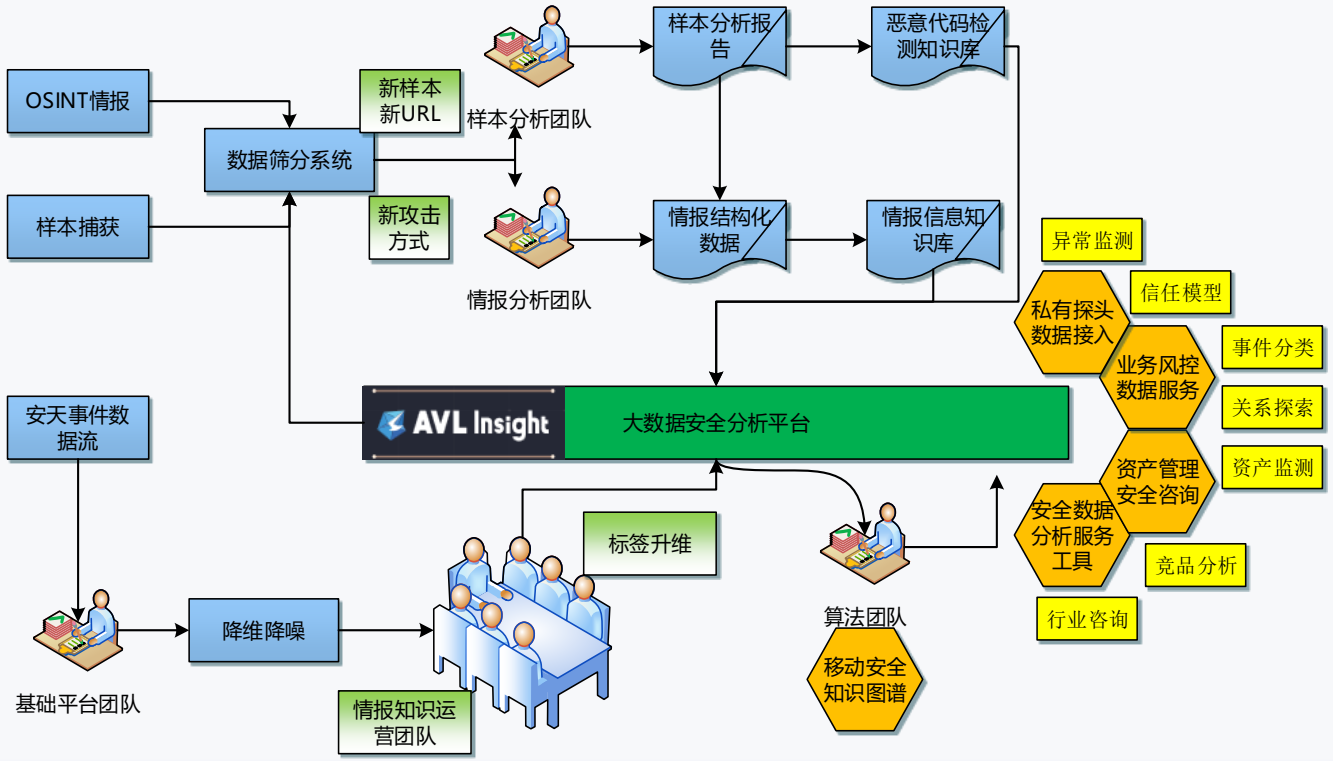
- 高可用性
- 高扩展性
- 高移植性



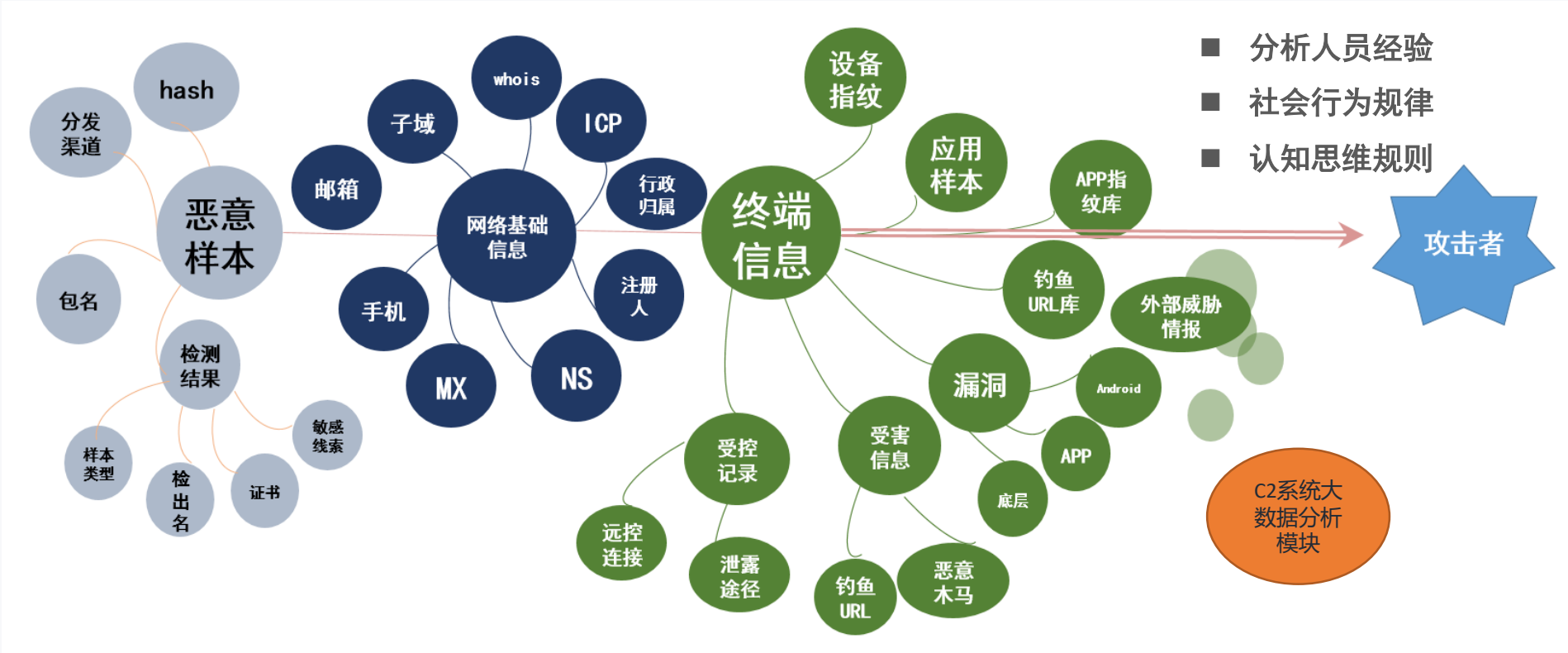
3. 面向服务的大数据分析模块设计



4. 信息域—认知域—社会域联动的多维情报拓展逻辑



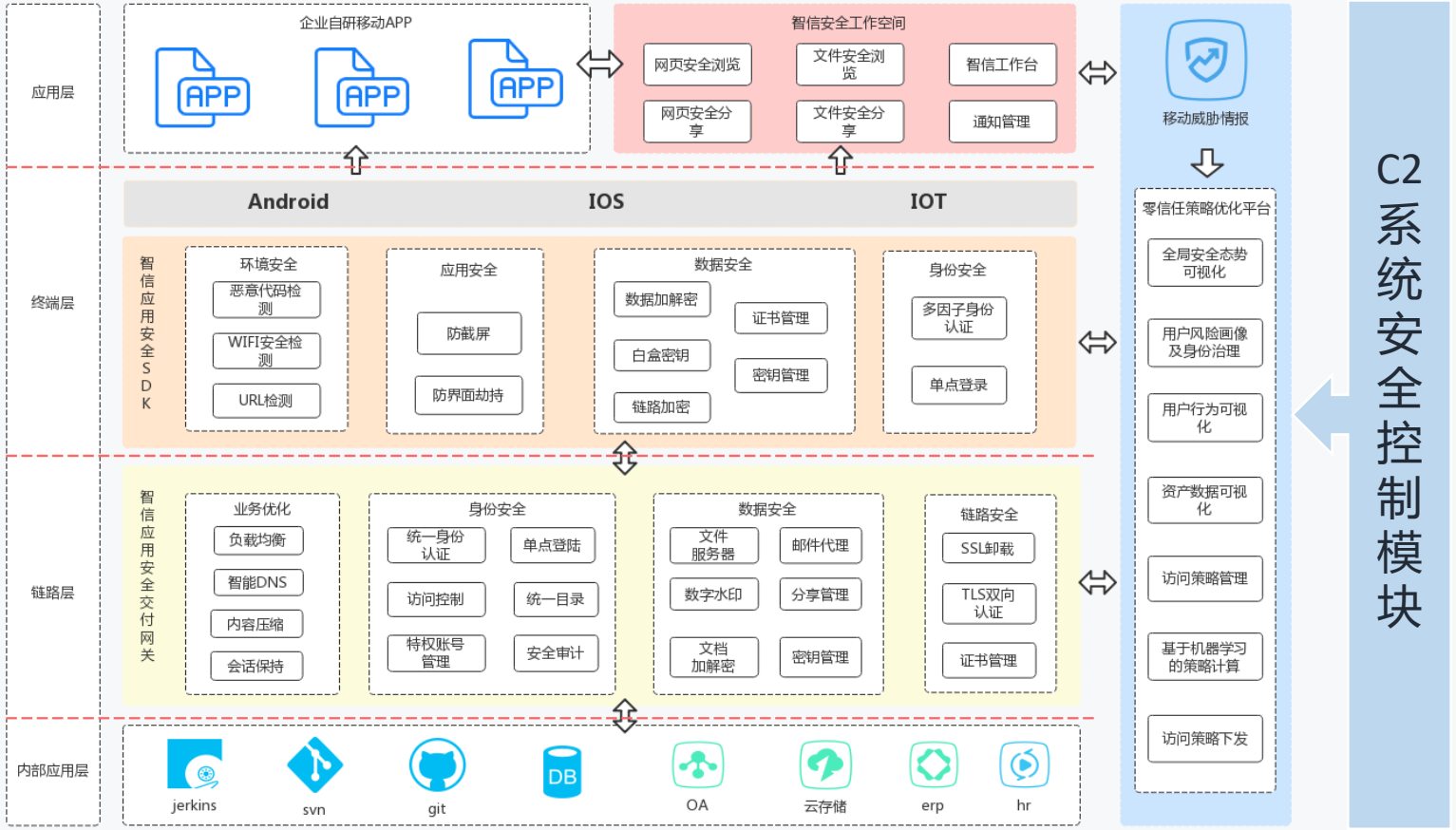
4. 信息域—认知域—社会域联动的多维情报拓展逻辑



5.零信任策略开启数据防护新实践

C2系统零信任模块基于端管云的体系架构，解决用户内部应用安全访问的问题，通过安全工作空间或sdk保障终端安全，通过应用安全交付网关保障用户内部应用服务的访问安全，通过零信任策略优化平台提供应用访问控制策略的动态计算能力，同时结合安全移动威胁情报能力，进一步增强应用访问的异常判定及访问控制策略的动态调整，从而全方位的保障应用访问的整体安全性，实现应用访问全生命周期安全的可靠、可控、可视、可查。

5.零信任策略开启数据防护新实践



第四章 PART THREE

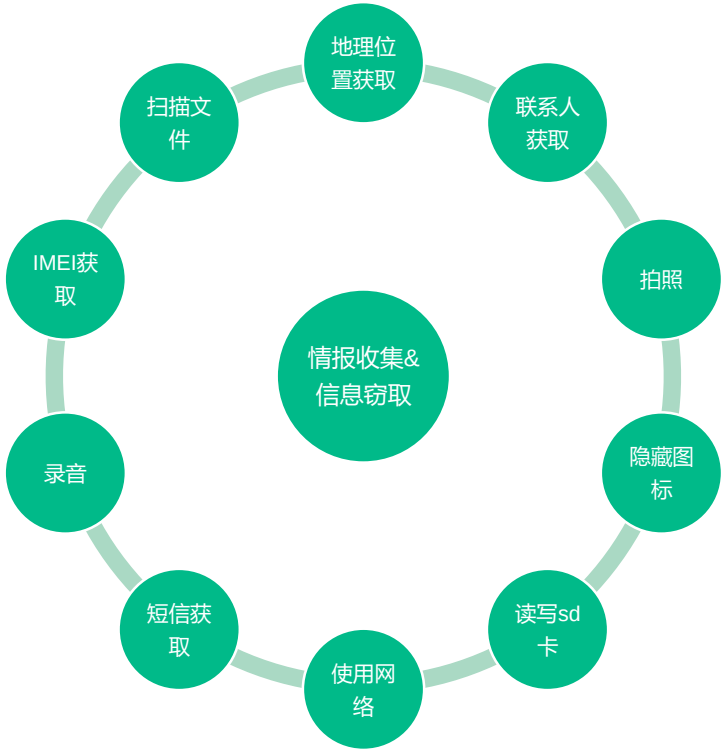
4

网络威胁情报分析案例实践分享

网络威胁情报分析案例实践分享

从样本载荷视角来看移动APT

高情报价值样本的形为模型



结合指挥控制系统理念的网络威胁情报分析与实践

统筹整合资源

Thanks

谢谢关注!