NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

拯救应急：
新一代网络安全能力建设之应急响应

杜跃进

网络安全应急技术国家工程实验室 主任
国家网络信息安全技术研究所 所长
国家互联网应急中心 副总工

2013.11.8 武汉

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

引言：为什么讨论这个话题

- 我们的网络安全能力面临严重挑战
  - *Stuxnet-Duqu-Flame：我们的发现能力、分析能力、应急能力？*
  - *网络战威胁：我们的“知彼能力”？*
  - *2009暴风影音事件、2013中国域名受攻击事件：我们的“知己能力”？*
  - *斯诺登事件、棱镜事件：我们的安全防护能力？*
- 成绩已经成为过去，国家网络安全能力需要重新调整，适应新型网络安全对抗形势
- 应急怎么做？Response - Readiness?

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

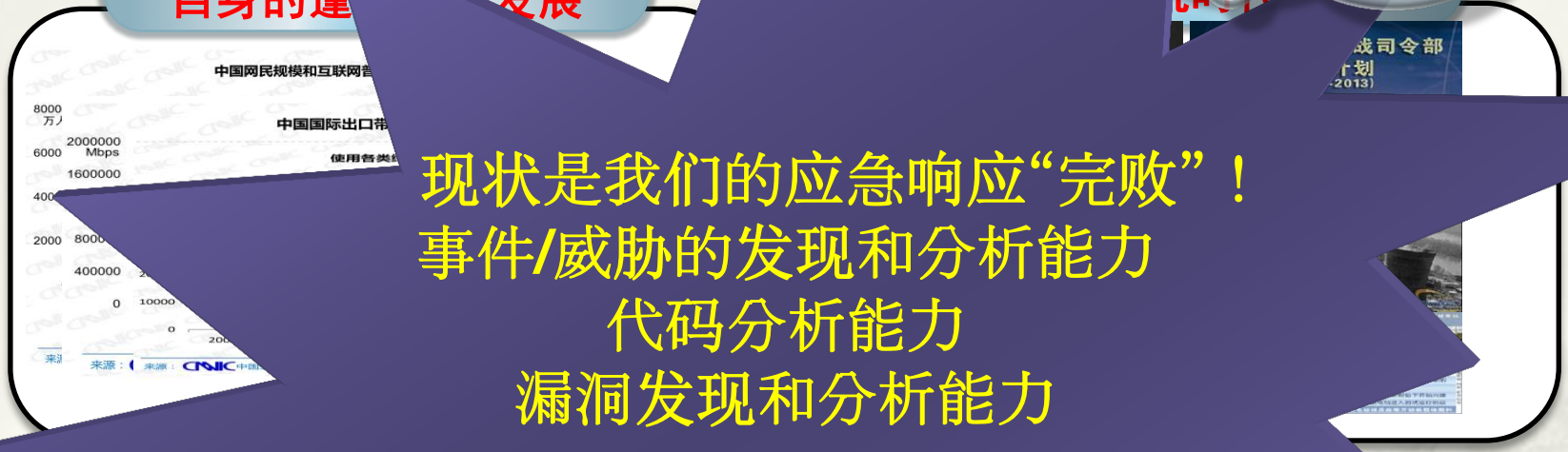
需求分析：形势严峻

2013年6月24日

互联网作为日益重要的国[illegible]础设[illegible]

面临严峻安全形势

自身的蓬[illegible]速发展



现状是我们的应急响应“完败”！

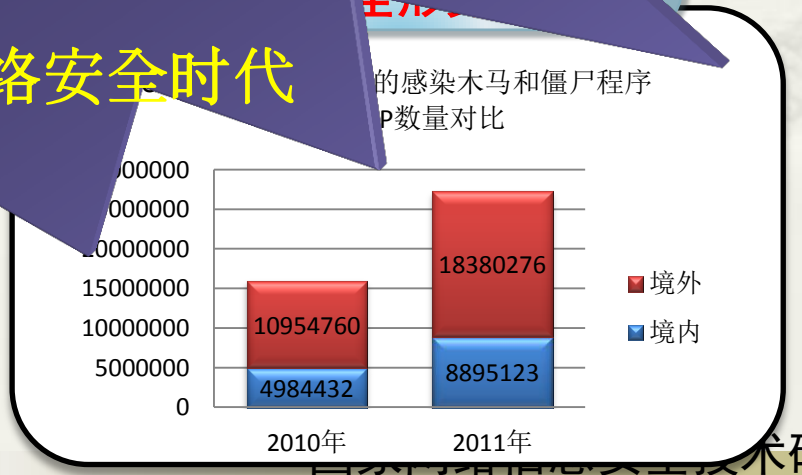
事件/威胁的发现和分析能力

代码分析能力

漏洞发现和分析能力

……

不适应新的网络安全时代



NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

内 容

换个角度看概念

问题出在哪里

新思路和新工作

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

“事件” ？ “威胁” ？

木马病毒	信息泄露	经济损失
网页篡改	密码破解	黑客大战
僵尸网络	产品漏洞	拒绝服务
网络钓鱼	系统入侵	系统瘫痪

技术人员容易理解狭义的事件

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

公众/用户容易理解的事件

* 棱镜门
* 暴风影音
* 用户数据大泄露
* 网络瘫痪
* ……
* 银行故障
* 经济损失
* 信誉损失
* 公司倒闭
* ……

影响和损失

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

“威胁”怎么理解？

- 事件强调已经发生的
- 威胁更强调潜在的“势”，涉及更多来源、动机、危害性的关注
- 威胁可能由多个事件造成，而且其中可以包括不同技术类型的事件（*APT 不是API*）
- 事件的应对主要是发现和处置（阻止、清除等）
- 威胁的应对需要更多的全面分析和评估

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

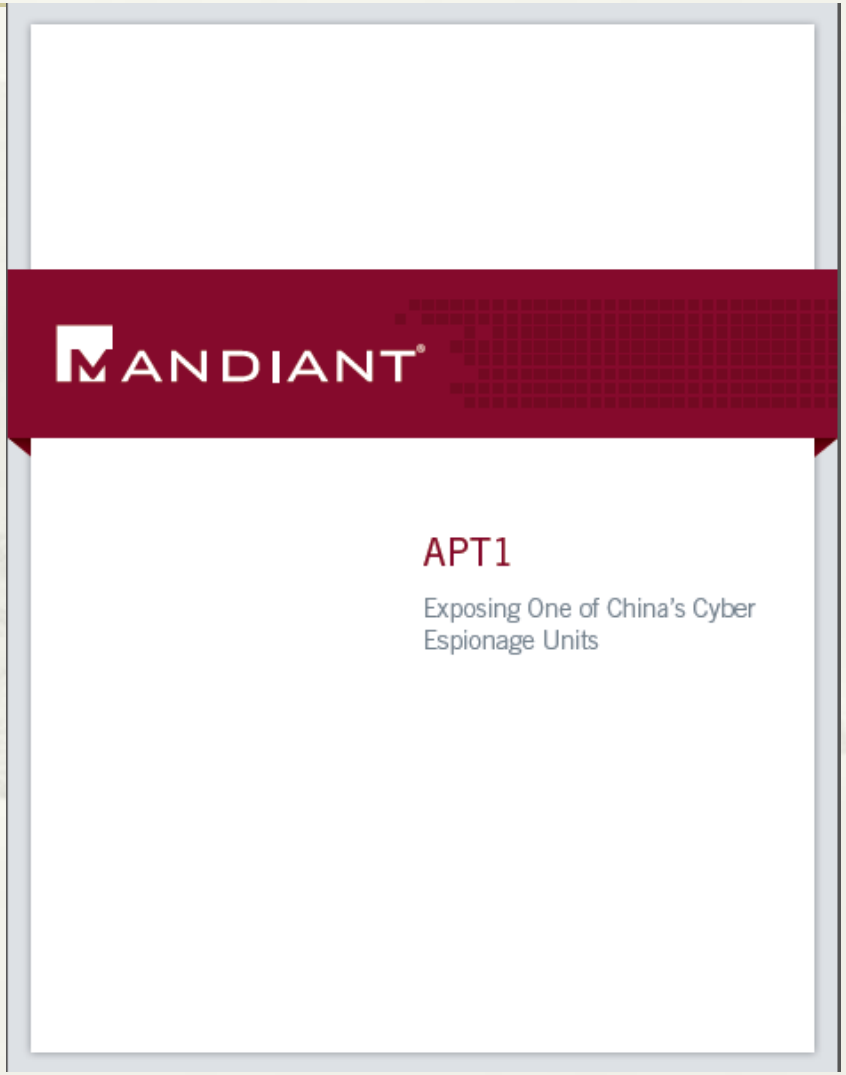
我们的安全报告主要围绕事件

* 被控制的IP、网站
* 发现多少漏洞、恶意代码
* 发现多少拒绝服务攻击
* ……

NINIS
NATIONAL INSTITUTE OF NETWORK AND INFORMATION SECURITY

别人的安全报告开始围绕威胁

* 什么组织
* 可能是什么人
* 在什么地方
* 做了什么事情
* 造成多大危害
* ……



NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

不同之处？

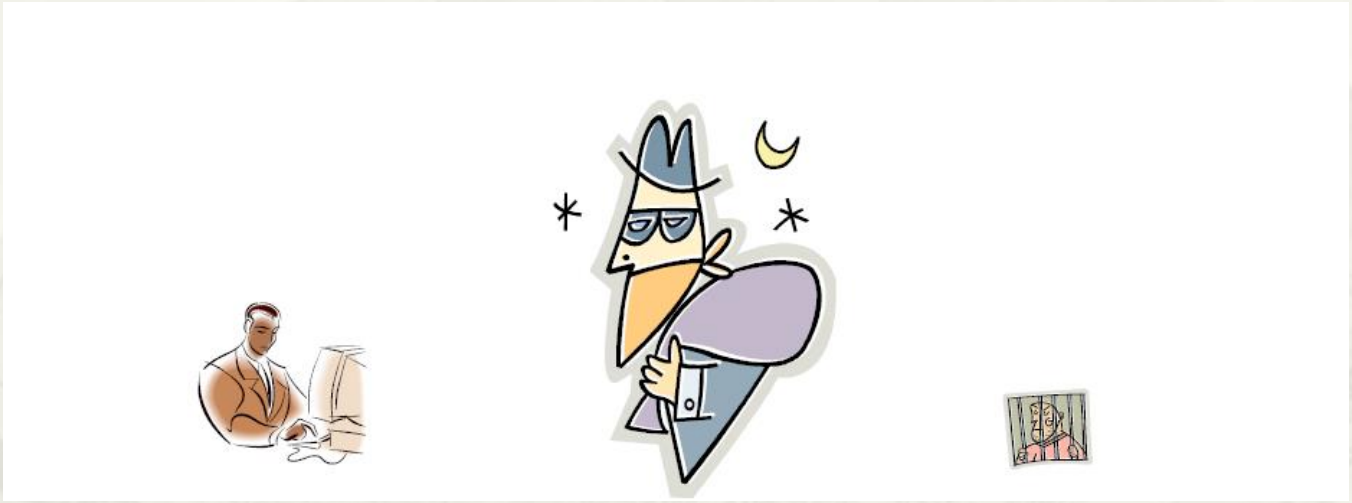
Payload

- Payload determines the desired result of an intrusion.
- If attack
  - Alter or erase files
  - Consume computing power to make computer slower
  - Assume control of connected devices
  - Change signatures on files
- If exploitation
  - Scan traffic passing by
  - Copy information, transmit copied to dead-drop site for later retrieval
  - Map connections
- If “preparing the target”
  - Provide “hook” for later access
  - Provide remote upgrade capability
  - Provide means for clandestine access by human operator who pretends to be authorized user.

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

我们应该应对的是什么

* 仅仅应对“事件”，越来越被动



* 面对高级安全威胁，这种做法必然失败
* 技术以外的因素，需要区分动机和目的

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

内 容

换个角度看概念

问题出在哪里

新思路和新工作

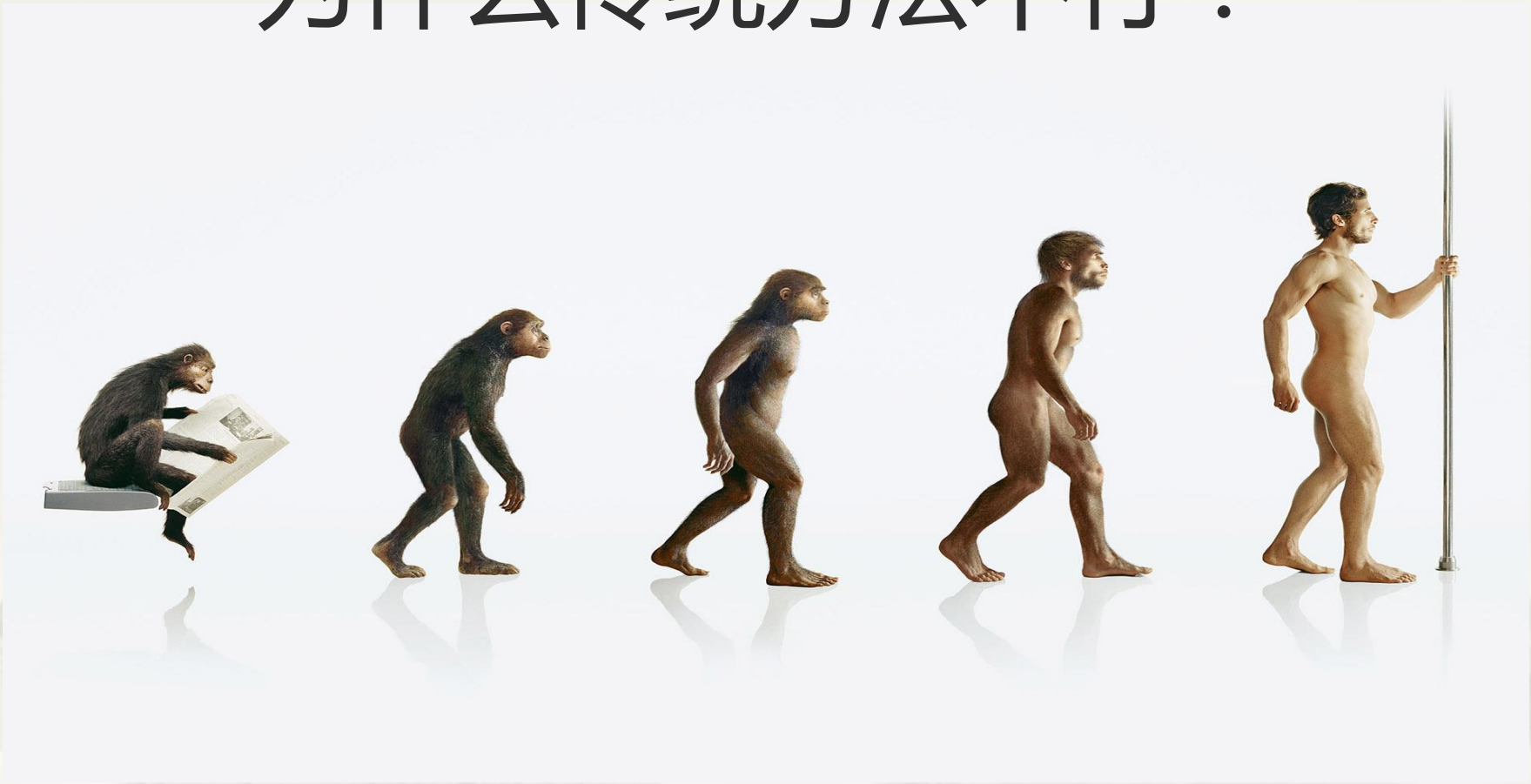
NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

现有技术能力的发展和问题

* 我国的国家网络安全事件发现能力的发展
  * 2001：蠕虫
  * 2003：木马、网站
  * 2005-：僵尸网络、VDS、蜜网、域名、流 etc
* 效果？
* 不足？
* 问题
  * 高位监测的问题，类似于NIDS的问题

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

为什么传统方法不行？



Signature, Traffic Behavior, Reputation, Cloud, ……?

现有思路的问题

- 过去的模式并不适用于新的安全阶段
  - 对新型威胁的认识不足
    （安全模型的第三维）
  - 对威胁和事件的理解偏差
    （没有提升到威胁，关联分析依然停留在事件的层面，没有真正的深度分析）
  - 对如何解决问题的理解偏差
    （事件处置 vs 威胁消除）
  - 对技术和设备的过度依赖
    （对抗的本质性认识问题）
- 需要建立新的思路

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

内 容

换个角度看概念

问题出在哪里

新思路和新工作

需要解决什么问题

- 溯源和动机分析
- 溯源的三个层面：
  - 主机（IP地址、机器）
  - 个人（操作者、自然人）
  - 机构（组织机构、负责任者）
- 三种可能的途径

需要的是全球层面的溯源

需要解决什么问题-续1

隐患发现和消除能力

* 高级安全性测试方法和环境
* 大型复杂系统的安全风险评估
* 大型复杂系统的安全性测试
* 第三方的产业链安全监督与测试
* 安全开发技术和管理
* 相关的知识库

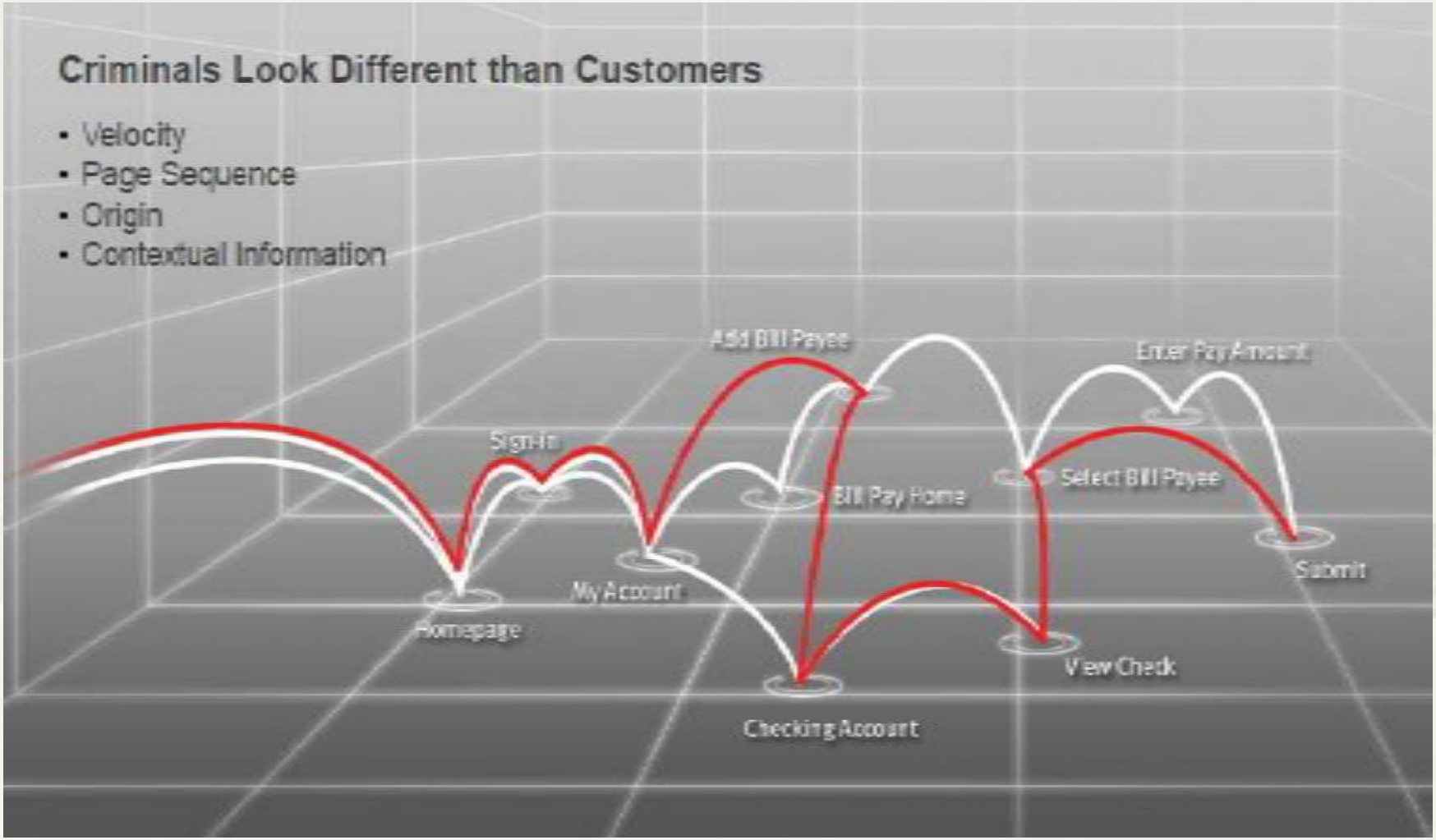
需要解决什么问题-续2

威胁发现与评估能力的提升

- 高位监测能力先天不足的弥补
  - “高位+目标知识”？
  - “高低位结合”？
- 多维度事件关联能力
- 威胁的评估能力和应对方案推演能力
- 威胁的（极早期）预警能力
- 未知攻击方法的感知与调查能力
- *[NIDS改进的方向？DPI和面向应用层的防护？]*

NINIS
NATIONAL INSTITUTE OF NETWORK AND INFORMATION SECURITY

未来安全能力：异常发现



NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

未来的安全能力：基于知识

* 并非仅仅围绕安全数据建立的知识
* 国家级知识体系的建立
  * 数据和信息的获取与更新
  * “带外知识”的整合
  * 流量模型的持续采集
  * 专业化知识库的持续分析与更新
* 知识辐射能力的建立

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

未来安全能力：深度分析与测试

- 尖端的安全性测试方法研究和能力建设
- 综合的深度分析
  - 恶意代码和漏洞
  - 安全事件
  - 综合数据

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

小 结

- 对事件的应急响应不同于对威胁的应对
- 国家网络安全能力面临空前挑战，需要重构
- 未来的能力是一种集成的、多方面能力的综合，并不是靠某一个大型系统的独立能力
- 新的能力需要多方参与，需要力量的凝结

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

ONE MORE THING

Something we can do

TOGETHER

国家网络信息安全技术研究所

围绕国家需求，研制实验平台；
基于实验平台，开展技术研发；
通过技术研发，支撑相关工作，提升国家水平

国家发展改革委办公厅关于请组织申报信息化领域创新能力建设专项的通知

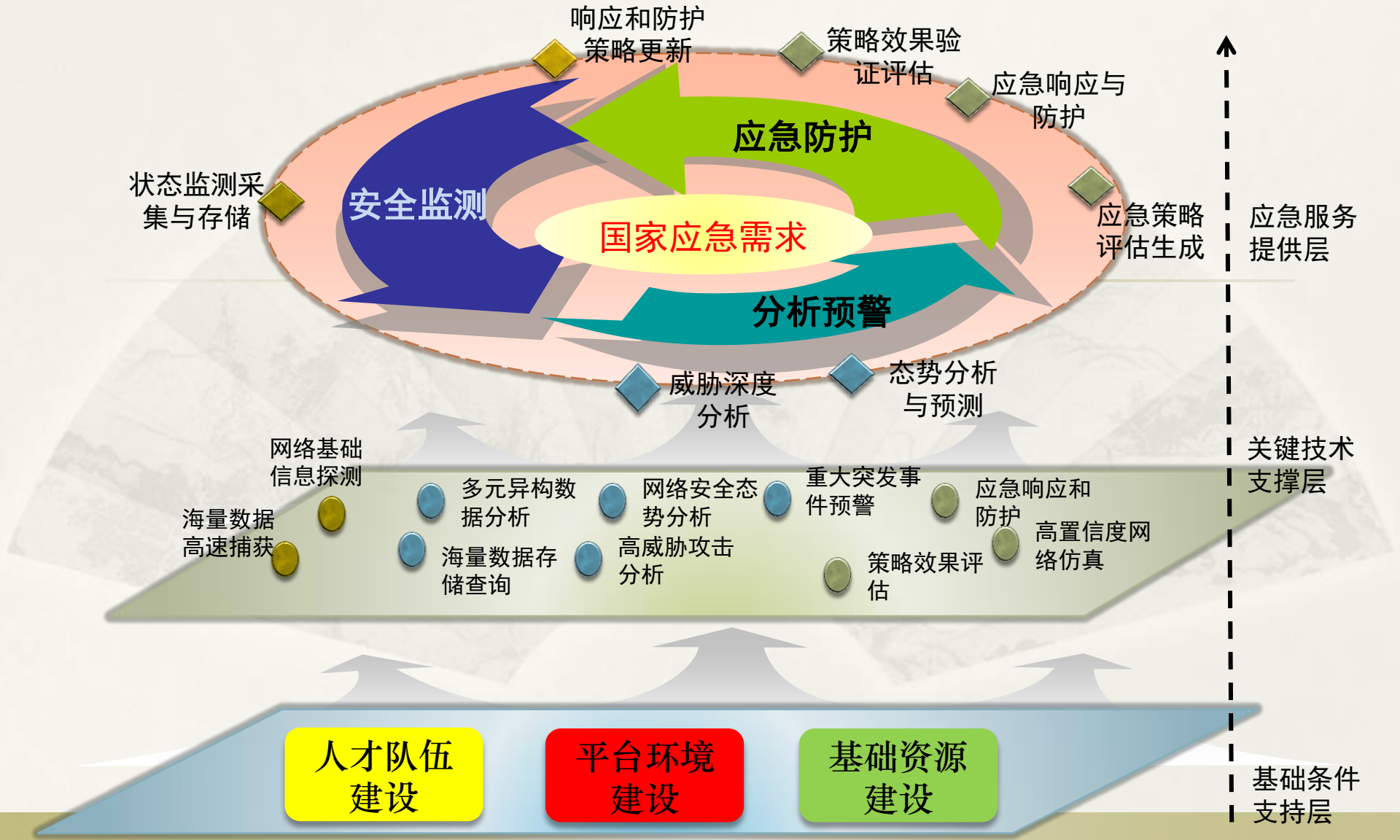
（二）信息安全方面

1、网络安全应急技术国家工程实验室

针对重大突发网络和信息安全事件预警、分析、处置的需求，建设网络安全事件安全防护、监测预警和应急处置的实验平台，研究数据高速捕获查询、海量存储、数据信息挖掘等大规模网络安全应急的重大技术问题，开展国家级网络安全监控体系建模、重大突发网络安全事件实时监控和网络安全态势分析预测关键核心技术研发，以提升国家网络安全应急工作水平，为保障国家信息基础设施，重要信息系统安全稳定运行提供技术支撑。

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

总体思路



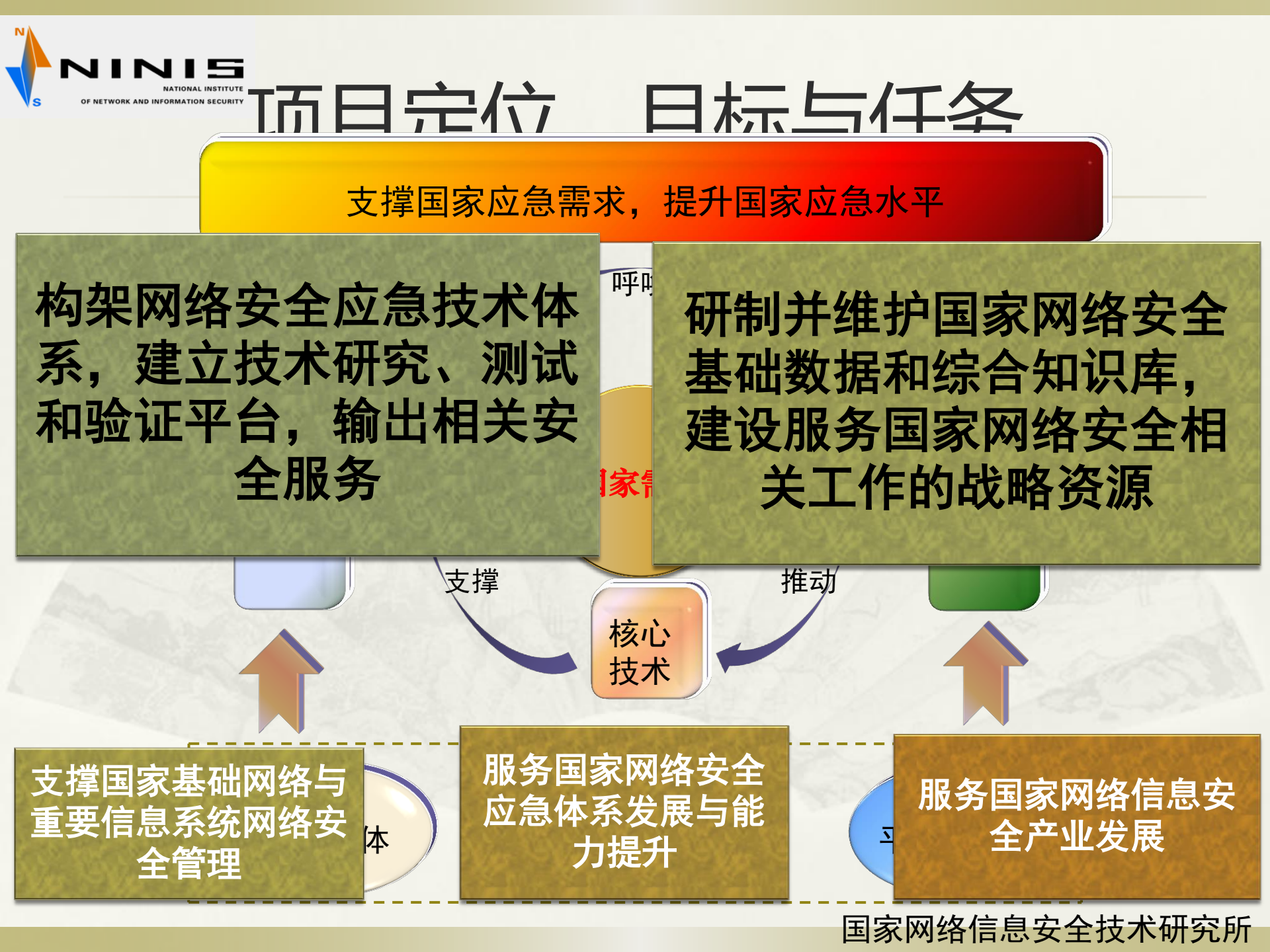
NINIS
NATIONAL INSTITUTE OF NETWORK AND INFORMATION SECURITY

项目定位 目标与任务

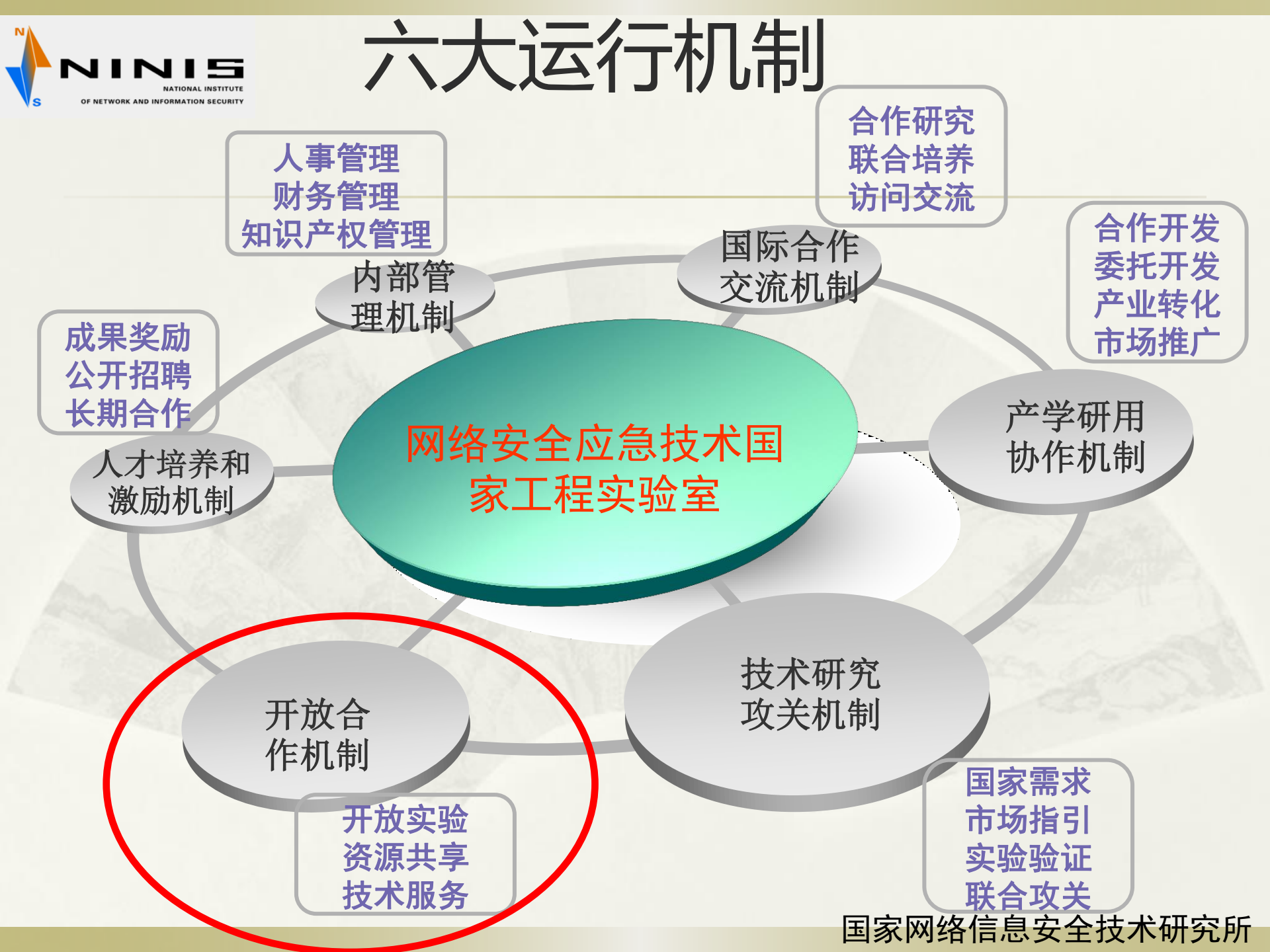
支撑国家应急需求，提升国家应急水平

构架网络安全应急技术体系，建立技术研究、测试和验证平台，输出相关安全服务

研制并维护国家网络安全基础数据和综合知识库，建设服务国家网络安全相关工作的战略资源



六大运行机制


网络安全应急技术国家工程实验室
内部管理机制
人事管理
财务管理
知识产权管理
国际合作交流机制
合作研究
联合培养
访问交流
产学研用协作机制
合作开发
委托开发
产业转化
市场推广
技术研究攻关机制
国家需求
市场指引
实验验证
联合攻关
开放合作机制
开放实验
资源共享
技术服务
人才培养和激励机制
成果奖励
公开招聘
长期合作

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

国家网络信息安全技术研究所