



新技术环境下的网络安全防护

蒋爱平

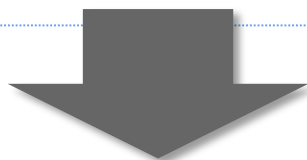
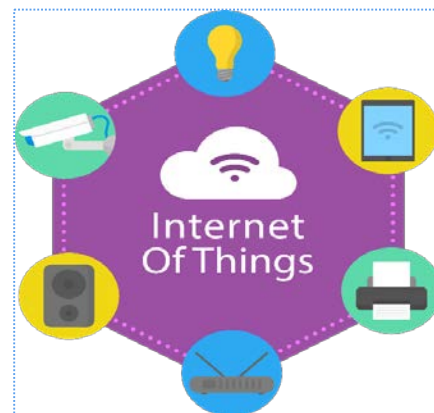
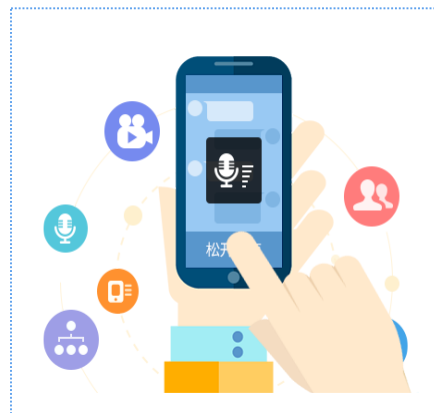
奇安信集团 战略咨询规划部

目录

新技术环境下的网络安全挑战

新技术环境下的网络安全体系

新技术环境下的网络安全挑战



数字化转型

互联网+
智慧城市
数字中国
网络强国



工业互联网

新一代信息技术加速突破应用，成为推动社会生产方式变革、创造人类生活新空间的重要力量。

变化的战场



变化的打击目标



变化的对手

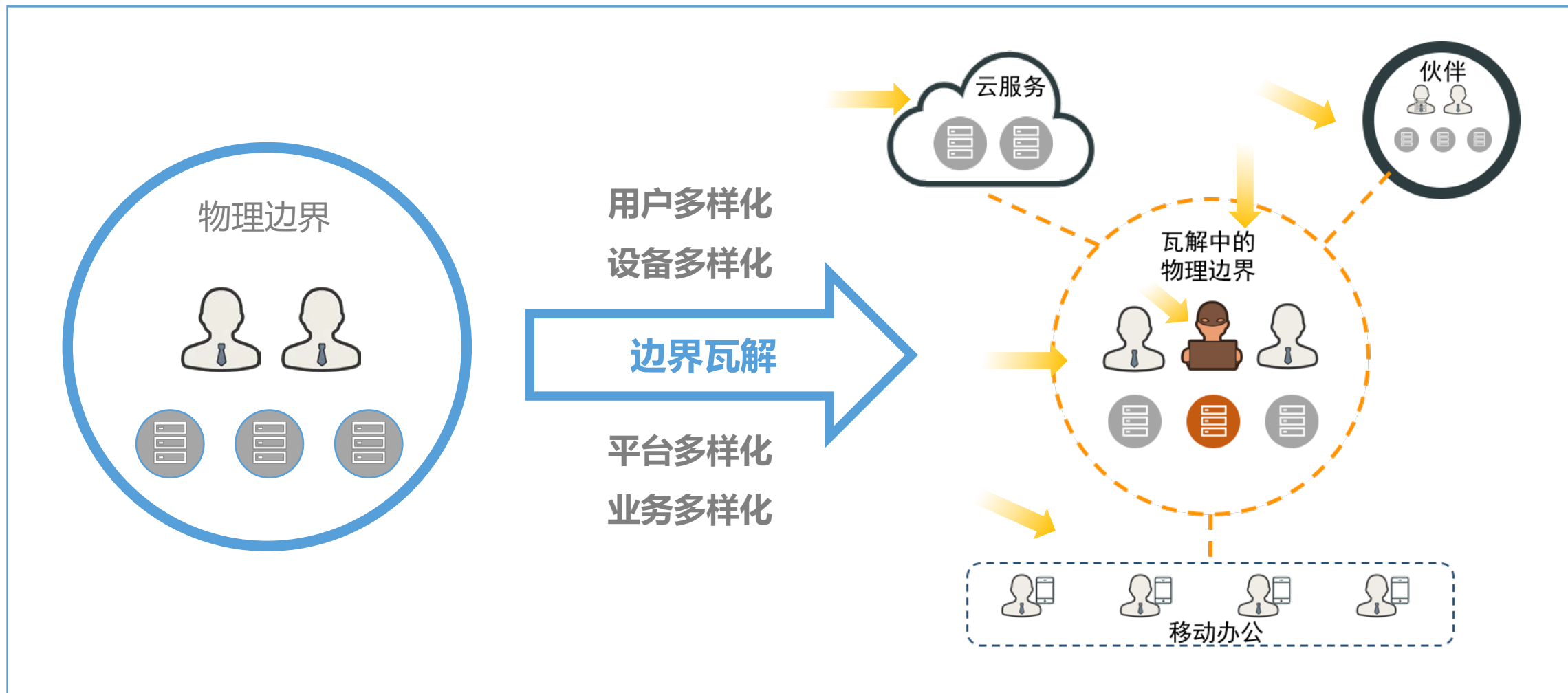


变化的武器与战术



变化的指挥监管



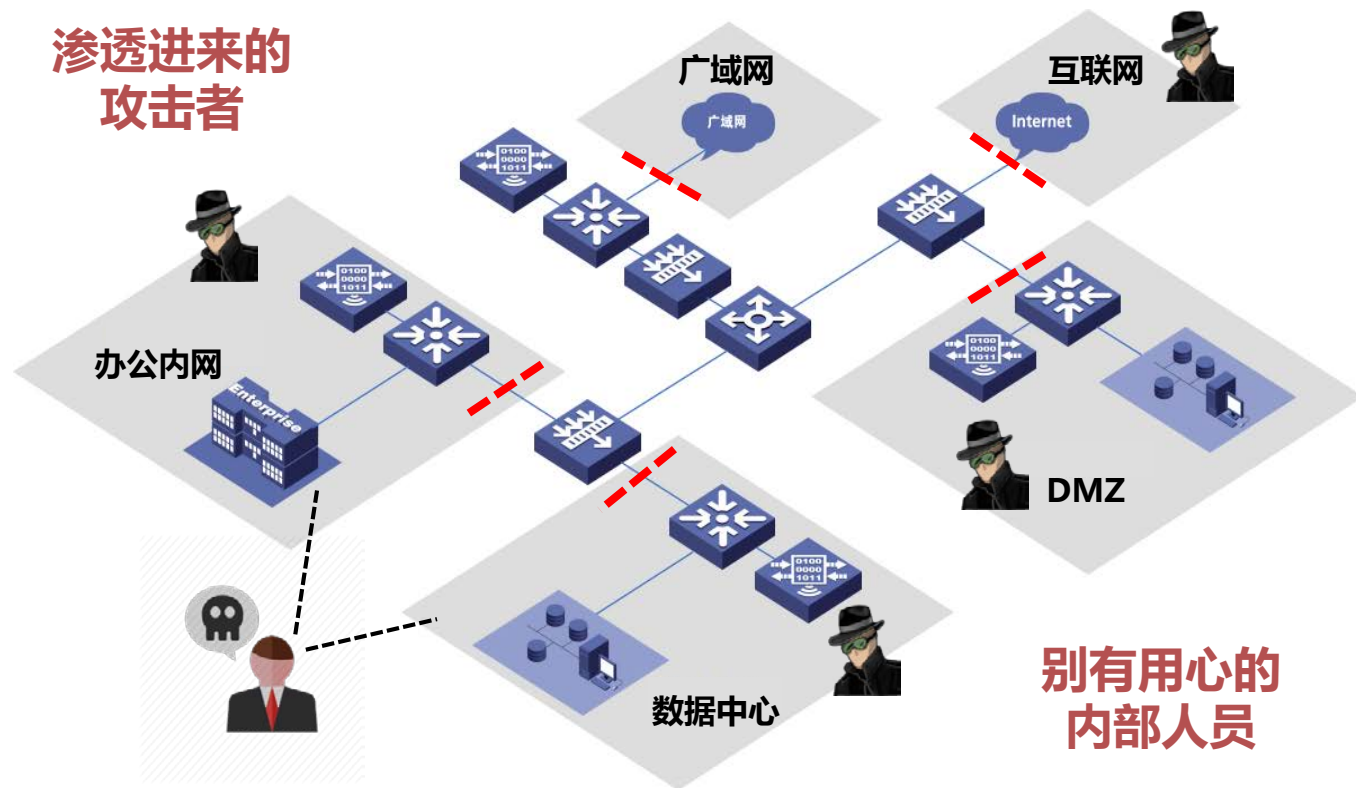


数据分散在不同的业务应用中并持续流动，流动加剧了大数据的风险

安全意识?

安全投入?

安全措施?



边界安全架构: 为内网中的人和设备预设了过多的信任



每一次数据泄露“黑天鹅”事件背后，都隐藏着“灰犀牛”式的危机。



目前奇安信累计监测到针对中国境内目标发动攻击的境内外APT组织39个，**窃取敏感数据**是APT攻击的主要企图，还有就是攻击**破坏关键基础设施**。

2018年公开高级威胁事件报告涉及行业分布情况

电信 3.3%
传媒 3.3%
医疗 3.3%
5.5%

针对我国的APT攻击愈演愈烈

- 国际形势冲突
 - 美国
- 地缘政治冲突
 - 朝鲜半岛/东南亚/南亚
- 台湾问题

| APT 组织 | 来源 | 最早活动 | 最近活动 | 主要目标 |
|----------------------|----|------|------|-----------------------|
| 索伦之眼 (APT-C-16) | 美国 | 2010 | 2016 | 科研教育、军事和基础设施领域, 水利、海洋 |
| 方程式 | | 2008 | 2015 | 基础设施 |
| Lazarus | 朝鲜 | 2009 | 2018 | 政府、金融 |
| Group 123 | | 2012 | 2018 | 电子、制造、航空航天 |
| Rocket | | 2017 | 2018 | 高新技术、外贸 |
| Darkhotel (APT-C-06) | 韩国 | 2004 | 2018 | 政府、科研 |
| 海莲花 (APT-C-00) | 越南 | 2012 | 2018 | 政府、科研院所、海事机构 |
| 摩诃草 (APT-C-09) | 印度 | 2009 | 2018 | 政府、外交 |
| 毒云藤 (APT-C-01) | 台湾 | 2007 | 2018 | 政府, 军事, 科研 |
| 蓝宝菇 (APT-C-12) | | 2008 | 2018 | 政府、外交、高校、科技 |
| 蔓灵花 | 未知 | 2013 | 2016 | 政府、电力和工业 |

新技术环境下的网络安全体系

四个假设

系统一定有没发现的漏洞
一定有已发现漏洞没打补丁
系统一定可以被渗透
内部人员一定会犯错

以“四个假设”
为前提保障网络
安全

四新战略

新战具：第三代网络安全技术
新战力：数据驱动安全
新战术：零信任架构
新战法：人+机器安全运营

以“四新战略”
为原则设计安全
方案

三位一体

高位能力
中位能力
低位能力

以“三位一体”
方法搭建安全
体系

三同步

同步规划
同步建设
同步运营

以“三同步”
思想做好体系
化保障

三方制衡

用户
云服务商
安全公司

以“三方制衡”
机制构建综合
高效系统

假设一

- 系统一定有还没被发现的漏洞

假设二

- 一定有已发现但未修补的漏洞

假设三

- 系统一定可以被渗透

假设四

- 内部人员一定会犯错

新战具



第三代“查行为”
网络安全技术

新战力



数据
驱动安全

新战术



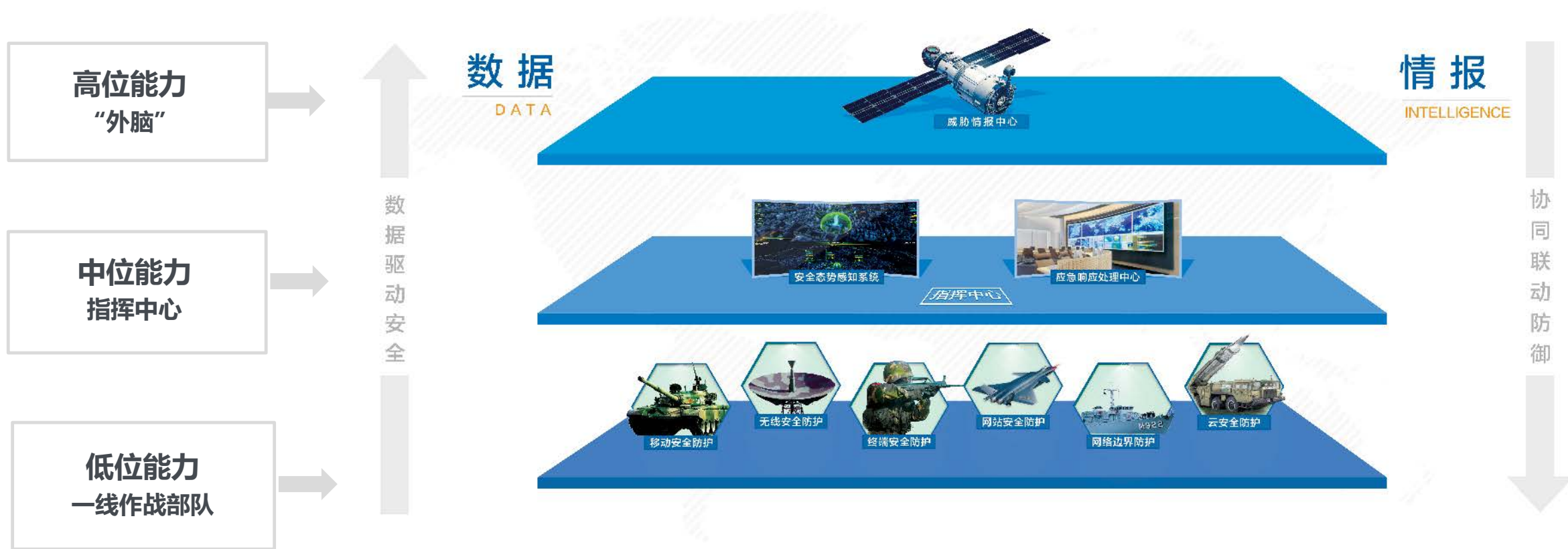
“零信任”
安全架构

新战法



“人机协同”
的安全运营

高位、中位、低位立体联动的一体化体系 实现从低到高的数据传送、从高到低的情报指令



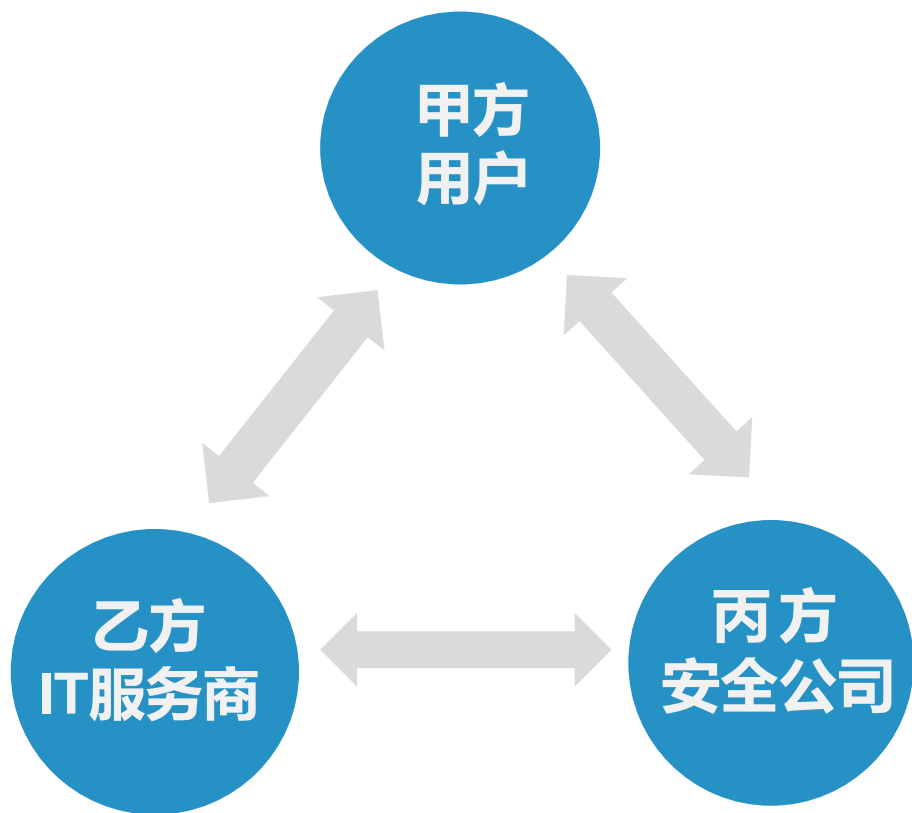
同步规划、同步建设、同步运营

从信息化的起始阶段，就充分考虑安全问题


做好横跨网、云、数据、应用、各种智能系统的体系化保障



云、大数据和IOT等信息系统的基础都是数字化信息，像安全“黑洞”
引入第三方的安全公司，对IT服务商形成有力制衡，真正对用户安全负责



- 甲方用户**严格要求**
- 乙方IT服务商**提高标准**
- 丙方安全公司**查漏补缺**
- 三方互相制衡，才能从最大程度上杜绝漏洞，长治久安。

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE