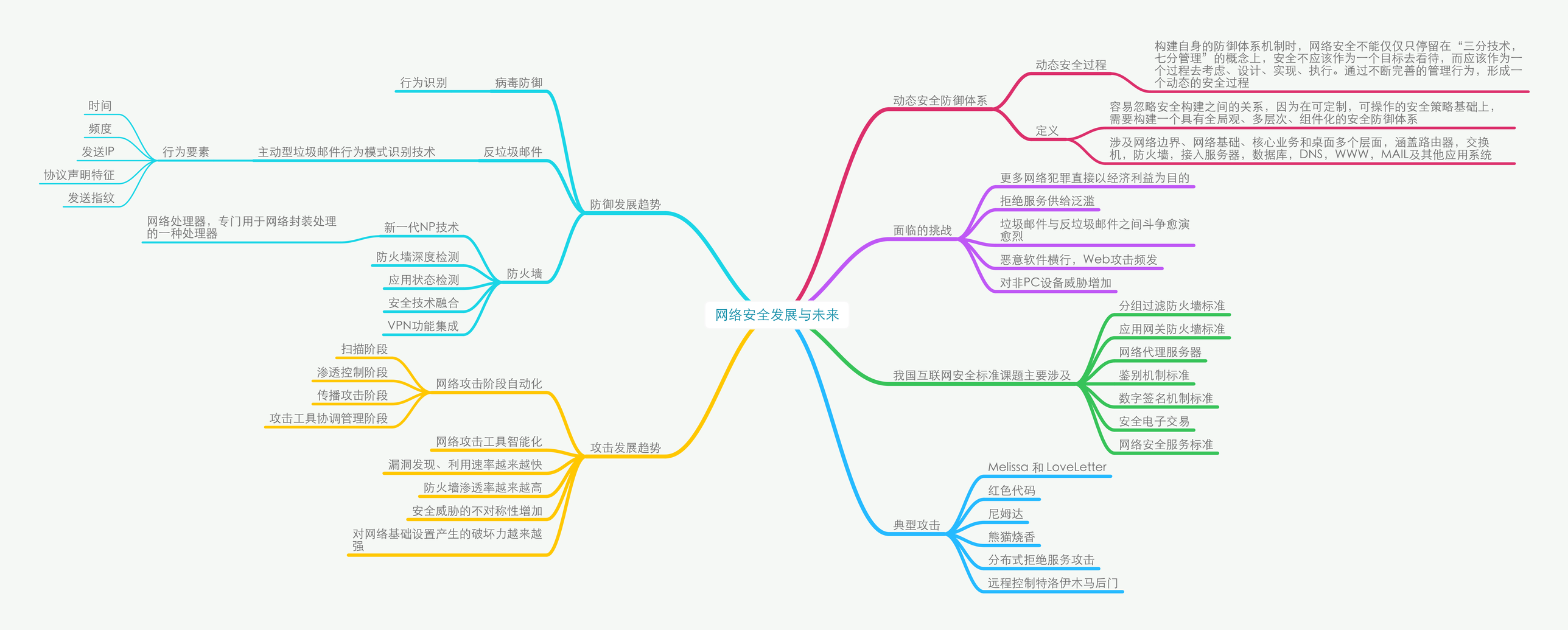
网络安全发展与未来
防御发展趋势
病毒防御
行为识别
反垃圾邮件
主动型垃圾邮件行为模式识别技术
行为要素
时间
频度
发送IP
协议声明特征
发送指纹
防火墙
新一代NP技术
网络处理器，专门用于网络封装处理的一种处理器
防火墙深度检测
应用状态检测
安全技术融合
VPN功能集成
攻击发展趋势
网络攻击阶段自动化
扫描阶段
渗透控制阶段
传播攻击阶段
攻击工具协调管理阶段
网络攻击工具智能化
漏洞发现、利用速率越来越快
防火墙渗透率越来越高
安全威胁的不对称性增加
对网络基础设置产生的破坏力越来越强
动态安全防御体系
动态安全过程
构建自身的防御体系机制时，网络安全不能仅仅只停留在“三分技术，七分管理”的概念上，安全不应该作为一个目标去看待，而应该作为一个过程去考虑、设计、实现、执行。通过不断完善的管理行为，形成一个动态的安全过程
定义
容易忽略安全构建之间的关系，因为在可定制，可操作的安全策略基础上，需要构建一个具有全局观、多层次、组件化的安全防御体系
涉及网络边界、网络基础、核心业务和桌面多个层面，涵盖路由器，交换机，防火墙，接入服务器，数据库，DNS，WWW，MAIL及其他应用系统
面临的挑战
更多网络犯罪直接以经济利益为目的
拒绝服务供给泛滥
垃圾邮件与反垃圾邮件之间斗争愈演愈烈
恶意软件横行，Web攻击频发
对非PC设备威胁增加
我国互联网安全标准课题主要涉及
分组过滤防火墙标准
应用网关防火墙标准
网络代理服务器
鉴别机制标准
数字签名机制标准
安全电子交易
网络安全服务标准
典型攻击
Melissa 和 LoveLetter
红色代码
尼姆达
熊猫烧香
分布式拒绝服务攻击
远程控制特洛伊木马后门