CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

超越合规视角的安全治理框架

宇宸

CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

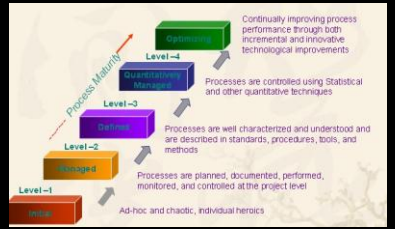
1. 网络安全能力模型

2. 从不同维度关注安全

3. 网络安全维度能力建设

网络安全能力模型

网络安全能力模型



Global Cyber Security Capacity Centre
Capacity Maturity Model

全球网络安全能力中心能力成熟度模型（GCSCC CMM）的首个版本出版于2014年，2017年更新为最新版本。国家的网络生态系统被认为由五个维度构成：

D1 –网络安全政策和战略

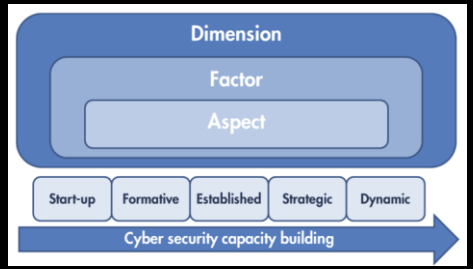
D2 –网络文化与社会

D3 –网络安全教育、培训和技能

D4 –法律和监管框架

D5 –标准、组织和技术

网络安全能力模型



兰德公司于2018年8月发布报告《发展网络安全能力》（Developing Cybersecurity Capacity），旨在促进国家级网络安全能力建设计划以及整体政策和投资战略的制定，以应对网络领域的挑战。报告中，对国家网络成熟度进行了详细的审查和评估，并将其结论更好地转化为切实的政策建议和投资战略，使政策制定更好地增强该国的网络安全能力。

从不同维度关注安全

从不同维度关注安全

D1 网络安全政策和战略维度

D1.1 - 国家网络安全战略
D1.2 - 安全应急响应
D1.3 - 关键基础设施保护
D1.4 - 危机管理
D1.5 - 网络防御
D1.6 - 通信冗余

D2 网络文化与社会维度

D2.1 - 网络安全心态
D2.2 - 对互联网的信任和信赖
D2.3 - 用户对于线上个人信息保护的理解
D2.4 - 报告机制
D2.5 - 媒体和社交媒体

D3 网络安全、教育、培训与技能维度

D3.1 - 意识提升

D3.2 - 网络安全教育框架

D3.3 - 专业培训框架

D4 法律法规框架维度

D4.1 - 法律框架

D4.2 - 刑事司法系统

D4.3 - 以打击网络犯罪为目的的正式/非正式合作框架

D5 标准、组织和技术维度

D5.1 - 遵守标准

D5.2 - 互联网基础设施的弹性

D5.3 - 软件质量

D5.4 - 技术安全控制

D5.5 - 密码控制

D5.6 - 网络安全市场

D5.7 - 责任性披露

网络安全维度能力建设

D1.1 - 国家网络安全战略

侧重于制定、审查和更新国家网络安全战略的能力，有助于确定网络安全行动的优先顺序，确定责任，并分配相关资源。

D1.2 - 安全应急响应

关注安全应急响应能力，特别是在国家层面上应对网络安全事件的能力。

D1.3 - 关键基础设施保护

强调保护那些对维持包括健康、安全、保障、经济和社会福利在内的重要社会职能所必需的资产和系统的能力。

D1.4 - 危机管理

着重强调发展国家建立、审查和更新国家危机管理程序、功能协议和标准的能力。

D1.5 - 网络防御

侧重于国家设计和实施网络防御战略的能力，同时保持对政府、国际商业团体和社会开放网络空间的好处和灵活性。

- 为网络防御战略指定一个核心任务所有者（负责人/负责机构）
- 进行风险评估，包括对威胁场景和现有漏洞的分析
- 制定网络防御战略
- 实施网络防御战略，根据取得的成果、威胁及作战环境的变化，持续审查并更新网络防御战略实施方法
- 制定网络防御原则
- 评估网络防御战略并进行改进

能力

- 被动网络防御
- 采购和供应链保障
- 应急响应
- 主动防御
- 核心网络防御中心
- 配套立法

组织

- 专业技能
- 设施
- 技术装备
- 内部结构

协调

- 鼓励公私合作
- 安全交流平台
- 角色与责任
- 与国际盟友及合作伙伴的适当合作
- 攻击性网络作战
- 网络情报
- 网络威慑
- 国内网络紧急响应

D1.6 －通信冗余

关注各国政府识别、详细规划和利用国家利益相关方之间的数字冗余和冗余通信的能力。

最后

- 分析问题应结合环境
- 安全治理是一个循环的过程

网络安全创新大会
Cyber Security Innovation Summit

THANKS