信息安全综合实践 课后作业一

《Cybersecurity Lessons Learned from the Pandemic》总结

一、内容总结

此文件的主题是从**疫情的流行**分析**网络安全**中面对危机及重大破坏的应对措施、预防手段。文中提到，应对疫情和重大网络攻击具有**全球性、测试治疗滞后性**等共性，同时要求各国通力合作、跨界响应，提出了**预防**远比仅仅基于发现和反应的战略更高效的防患于未然的思路。

全文分为两个部分：

第一部分"**大流行期间的网络安全挑战**"介绍了流行期间的应对措施，提出了在当前社会距离协议下更为紧迫的建议。具体涉及：1、关键服务的数字化和安全实现的需要；2、随着疫情期间在家办公的增加，政府应领导推动更安全可靠的网络生态系统；3、政府应加强打击机会主义网络犯罪的能力，惩处欺诈和其他恶意活动。

第二部分主要讲述了从大流行中可以反思**如何预防重大网络破坏**，并提高在必要时对重大网络攻击引发的危机作出反应的能力。具体涉及：1、国内和国际的战略领导和协调，建设网络安全基础设施；2、确保经济规划连续性，对危机所构成的风险具有深刻理解并在危机前以数据驱动的方式降低风险；3、政府领导需要有应对和恢复能力，提供关键资源并随时恢复正常生产生活，包括事先规划、协调政策应对。

二、内容分析

下面我将就以下两点谈一谈我的认识分析：

1、物联网安全法的颁布完善

由于疫情防控需要，人们的大部分时间都在家中度过，居家办公使得个人设备、家庭网络一跃成为商业基础设施的核心组成，但现行法律中缺乏对**物联网设备和家庭网络安全的系统保护**。考虑到家庭网络已成为我们国家网络生态系统中敌人攻击面大且脆弱的一环（例如：Wi-Fi路由器的不安全性），广大物联网设备制造商在销售产品时应加入最基本的安全措施，例如普及国家网络安全认证，通过标识管理局颁布认证并扩大标识活动的范围，使得产品消费者的个人电子产品都能包括在内。在我看来，在广阔的物联网设备市场应引入。另外，在技术上减少引入漏洞的可能，提高系统安全性也能显著改善物联网生态环境。

同时，物联网设备还存在着大量**终端安全威胁**，例如：弱口令、身份认证识别弱、易被植入恶意代码等等。在完善法律的同时，物联网也需要在技术层面优化安全结构，防止身份伪造、API接口恶意攻击、DDoS攻击等问题的产生。

2、关键服务的数字化

疫情中公司不得不将业务转移到网上，员工们只能选择居家办公的模式，在这一大背景下，**安全、可靠的远程云服务**显得至关重要。在社会各个领域，**普及数字化**在短期内的成本异常高昂，这使得重视成本、缺少投资的中小企业难以企及，在追求短期资金优先的大环境下更是经常推迟服务的数字化进程。

数字化的优势不言而喻，它使程序更灵活，在提供服务方面能创造更高的效率和灵活性，并且可以提高服务提供商的安全性。事实上，考虑到**关键服务数字化**的高门槛，中小型企业以及国家、地方实体可以考虑采用集体安全和规模经济的形式，这样就不用独立地为安全解决方案和数字化进程付费，而是集中资源，建立更高效、有弹性的系统。

三、意见建议

1、基础安全领域投入较少

我们知道，广义的网络安全包括通用安全，专用安全，自用安全和基础安全四个方面。从我国目前的市场占额来看，很少有立足于**基础安全**的企业，更多的企业都选择从事通用安全，即数据安全、安全管理这些核心技术含量不高的产品业务。正如文中所说，国家需要**加大对关键服务的安全投入**，我们国家的关键信息安全基础设施行业也需要更多的资金和人才。

2、物联网安全领域法律保护不足、业务安全存在风险

物联网设备占据很大的市场份额，并且呈逐年上升趋势。然而，物联网设备往往没有配置相应的防护功能，同时大量的物联网设备也存在广泛的网络攻击入口，在面对恶意代码、DDoS攻击时缺乏保护手段。我们国家信息安全领域的法律逐步完善，但现阶段对于物联网设备的法律保护尚不够完善，对于入侵物联网设备的攻击行为、恶意利用没有严格界定和惩罚机制。

在技术层面可以对提出一些安全要求：**1、接入控制**：物联网设备接入时需保证只有授权设备允许被接入、限制节点通信的目标地址；**2、节点安全标识**：物联网需具备识别合法连接设备的能力，采用密钥、标识等方式拒绝非授权用户的访问；**3、制定统一的物联网通信协议标准**，对蓝牙、NFC等技术进行严格安全监控；**4、引入WAF和入侵检测模块**，提高安全性。