以“三化六防”措施构建网络安全综合防控体系

周佑源　柳少凯
（武汉安域信息安全技术有限公司，湖北 武汉 430077）

摘　要　网络安全问题已经得到社会各界的广泛关注，实现网络安全也成为社会发展的必然要求。文章从网络强国战略思想入手，围绕“三化六防”的相关问题展开深入讨论后，介绍了融合“三化六防”思路工作路径问题，提出了构建安全防护管理框架、主动发现网络安全问题的对策，旨在对全面贯彻落实“三化六防”思想，强化网络安全防控管理能力有所裨益。

关键词　网络安全　网络战　安全保护能力
中图分类号：TN915.08　　**文献标识码**：A　　**文章编号**：1007-0745(2022)10-0022-03

1 网络强国战略思想

网络安全事关国家主权、人民共同利益，事关国家安全。维护我国网络安全是实现“两个一百年”奋斗目标、实现中华民族伟大复兴中国梦的重要保障[1]。回顾近年来国家网络安全大事记，深入学习网络安全对贯彻落实国家战略布局与重要举措意义重大。国家网络安全保障体系健全完善，是有效消除潜在网络安全隐患、维护社会和谐稳定发展的重要组成部分，可以充分挖掘我国网络空间的潜力，使更多的居民享受到网络技术发展带来的便利，最终推动社会进步。

2016年12月27日，国家互联网信息办公室发布《国家网络空间安全战略》。

2017年6月1日，《中华人民共和国网络安全法》颁布实施，这是我国网络安全的“基本法”，是网络安全法律法规体系的核心。

2018年3月21日，中央网络安全和信息化领导小组改为中国共产党中央网络安全和信息化委员会。

2019年5月13日，网络安全等级保护制度2.0标准正式发布，国家对信息安全技术与网络安全保护迈入2.0时代。

《中华人民共和国数据安全法》于2021年9月1日起施行。

2 “三化六防”理念举措

2020年7月22日，公安部印发了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，指导意见明确要求要求重点行业以及相关部门能够高度认识到网络安全管理的重要性，并将其作为全面推动网络安全建设的重要一环，最终消除潜在网络安全隐患[2]。在新的时期，通过全面落实“四新”要求和“三化六防”新举措，成为发现网络安全隐患、主动处置网络安全问题的重要组成部分。

所谓“三化六防”是指“实战化、体系化、常态化”，“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”，以此构建国家网络安全综合防控系统，深入推进等保和关保的积极实践。根据指导意见明确要求，在贯彻落实等保和关保双制度，总体提出以下以等级保护为基础，突出关键信息基础设施保护、平台化安全运营服务理念。

2.1 网络对战视角看“三化”理念

“实战化、体系化、常态化”的内涵是非常丰富的，联系紧密有序，站在网络战的角度从“实战化、体系化、常态化”出发，构建网络空间综合防御作战体系。

第一，强调网络安全的“实战化”，攻防是网络安全的本质，习近平总书记指示网络安全的本质在对抗，对抗的本质在攻防两端的能力较量。未来的网络安全攻击将呈现高级化、大型化特点，网络战成为首选之一[3]。夺取并掌握“制网权”，一场没有硝烟的战争已悄然拉开序幕。从“震网”开启网络战新时代，世界各国成立网络作战部队，关键基础设施网络攻击愈演愈烈，成为国家当前不得不面对的严重问题。

第二，强调网络安全的“体系化”，从网络对战思想上，作战需要有部队，部队分不同军种，每一种军种要有特色打仗的武器，同时还要有多军种协同作战。作战还得有指挥调度平台，平台运作要有相关的保证。相对而言，网络安全对应网络安全产品使用、人员体系、领导决策、行业监管等均涉及多各方面，

缺一不可。

第三，强调网络安全的“常态化”，网络战隐蔽性强，网络作战时间不局限于白天或者夜幕，而是真正的全天候、全时域作战，网络潜伏和侦查早已进入战场，防护要求“常态化”，犹如当今时代以“和平与发展”为主题，更要有一种“居安思危”的意识，日常训练、对战演练等，加强国防建设具有极大的重要性。

2.2 网络安全能力看“六防”措施

“三化”可以理解为用户在网络安全方面的一种要求，而“六防”代表一种能力，是需要掌握和具体实现的。

1. 动态防御：相对而言，现阶段的网络安全问题呈现出明显的复杂态势，为了能够实现网络安全预防的目标，则需要工作人员能够从当前的技术手段出发进行网络安全风险防控，例如积极开展网络安全入侵检测、积极强化防火墙功能、做好病毒查杀等方法，上述一系列网络安全防控工作都可以在静态网络环境下进行，依托网络安全管理手段，在实现网络协议以及网络结构不变的基础上，快速发现潜在网络安全问题进行处置，例如系统可以直接识别有无网络入侵现象等，根据系统识别的结果可以针对性地采取网络安全控制，将网络安全控制在萌芽状态。动态防御则改变游戏规则，动态防御在网络安全管理上具有明显的灵活性特征，不会遵循传统生硬的网络安全管理模式，而是真正实现了网络安全控制的随机动态特征 [4]。

2. 主动防御：老旧的安全防护有防火墙、入侵检测、病毒防范被动防御模式，面对日益猖獗的安全威胁防不胜防。基于可信计算技术改变传统的网络安全管理模式，形成新的安全防控体系，在网络安全体系运行过程中能够结合威胁情报、态势感知，及时发现和处置未知威胁，落实主动防护措施。针对主动防御具有扰乱网络攻击的能力，部署二代蜜罐，进而诱导网络攻击行为，方便相关人员进行有效处理，并且由此造成的损失几乎可以忽略不计。

3. 纵深防御：施行分区域管理，区域间进行安全隔离和认证；实行事前监测，事中遏制及阻断，事后跟踪及恢复，实现攻击的层层狙击，全流程防御。纵深防御在电力行业信息系统防护层面得到借鉴，强调安全防护原则，在实现网络架构安全防护分区的基础上，加强“综合防护”的要求，内网建立安全监视，部署网络安全监测平台。

4. 精准防护：基于资产的自动化管理，协同威胁情报，检测未知威胁、异常行为等，实现对核心资产的精准防护，提供内生安全、主动免疫能力。在国内疫情防控上类似，精准打击妨害疫情防控犯罪，避免政策把握粗放化、简单化。网络安全防护也当如此，不能追求一概而论，同样也要精准发力，不能简单地“一刀切”。

5. 整体防护：以保护关键业务链为目标，进行整体安全设计，建立协同联动、高效统一的安全防护体系。改变传统单纯依靠强化局部网络安全管控能力来达到消除风险的效果，真正实现了从全局整体出发，提升事前、事中、事后的闭环运营。

6. 联防联控：建立与国家监管部门、保护工作部门、其他利益相关方的协调配合，联动共防机制，建设“打防管控”一体化网络安全综合防控体系，提升国家整体应对网络攻击威胁的能力。应积极融入网络安全整治，并与监管部门紧密合作，配合相关主管部门，共建联防联控的安全保护体系。

3 融合“三化六防”思路工作开展

3.1 以网络安全实战攻防，发现防护安全问题

问题都是被“打”出来的，安全经验偏重于“防”，通过近年来的护网总结的漏洞汇总情况来看，国家、省、地市或行业的实战攻防中，在告知攻击时间、限定攻击手段等前提下，攻破率（取得核心系统权限、获取核心敏感数据）一般在 30% 以上。而且针对产品服务厂商，特别是网络安全防护产品漏洞比重上升趋势。通过实战攻防和典型的安全事件，突出问题主要如下：

3.1.1 互联网资产梳理与暴露面收敛不全面

通过护网防守工作，在互联网层面资产梳理、暴露面收敛等是防守的一大关键要素。正如“你无法保护你看不见的东西”。随着基础设备的扩展和应用的接入，一些容易被忽视的弱点导致安全人员难以察觉，影子资产很容易成为漏网之鱼，往往这些资产责任防护落实不到位，存在漏洞修复不及时，导致被攻击利用的可能性增大 [5]。

3.1.2 供应链风险排查风险机制不完善

通过安全防控措施来看，往往在正面防护和防线严格，在抵御互联网正面网络攻击防护强度高，部署了大量的人员、技术、设备进行防护。在攻击方的角度，一个单位系统组织结构、直属单位带动供应商、设计单位、第三方单位等供应链伙伴错综复杂，这些供应商参与的信息集成、业务协作和资源共享，往往这些单位进行侧面攻击，同样给攻击方带来了多渠道化的攻击途径。

3.1.3 现有的安全防护被动、孤立和静态

通过多起勒索病毒安全事件，“钓鱼邮件”“口令爆破”“漏洞利用”攻击是最常见的三类攻击手段，从安全事件过程分析，勒索病毒的攻击往往从第一台设备感染，之后依托网络或者局域网等传输平台快速

散播病毒，并开始同时攻击业务系统以及服务器等，在连续的网络攻击下可能会造成系统瘫痪等严重问题，影响了正常的企业运营管理。从路径和过程分析，勒索病毒从 “互联网单台设备感染→扩散至内网核心数据服务器→数据备份措施失效→数据丢失导致业务无法恢复”的流程，说明其基础防护措施均没有落实到位。

3.2 以合规建设为基础，建立体系化防护框架

3.2.1 等级保护工作对象体系化

深入开展系统等级保护备案工作，全面对系统资产梳理，摸清家底，涉及的等级保护 2.0 工作对象包括基础信息网络、工控系统、云计算、物联网、移动互联和大数据平台等。科学确定网络的安全保护等级，经相关部门审核后依法向公安机关备案，并向行业主管部门报备。

3.2.2 安全建设和整改体系化

网络安全等级保护建设整改工作是开展等级保护工作的核心和落脚点，建设“一个中心”管理、“三重防护”体系，安全通用要求包括物理环境、安全便捷等多方面要求，并且随着网络系统功能的拓展，其完全管理的范畴被进一步扩大，包括物联网安全拓展以及工业控制系统等，都成为当前网络安全管理中不容忽视的问题 [6]。由此可见，现阶段的网络安全问题已经发生明显变化，其网络安全架构以及安全管理范围的增加都会明显提升安全管理的难度，对网络安全防护框架提出了更严格的要求。

安全通用模式下，网络安全管理需要从全局性入手，在了解保护对象形态的基础上快速形成网络安全管理对策。而在这个过程中，网络安全管理被赋予新的内涵，能够满足云计算、移动互联等网络架构的安全扩展要求。从技术方面：体现了从外部到内部，从边界到终端的纵深防御思想。对物理环境、基础网络、区域边界、计算环境、运营管控等的整体防护；从管理方面：网络安全管理中必须要从多个管理途径入手完成安全隐患的统一管理，这就需要相关人员能够认识到网络安全管理制度、安全管理策略等几方面因素的影响后构建统一的网络安全架构，并且网络安全管理内容也要充分考虑到未来安全体系功能拓展等几方面的要求，尤其是可以针对特殊安全管理对象展开多维度的网络安全控制，最终达到消除风险的目标。

3.2.3 监测预警通报体系化

针对各类网络安全事件展开预防控制是消除安全风险的重要手段，因此需要按管理要求向行业主管部门报告网络安全事件。依托技术支持单位、专家、社会资源，以及公安机关等完成安全预警。同时，用户在网络安全规划和建设中，需秉承“三化六防”理念措施，建立全面覆盖运维、开发、服务全场景的安全防护体系与安全运行流程，形成安全运行的体系化、标准化支撑，建立“人 + 技术（平台、数据）+ 流程”协同联动的防御模式，建立网络安全综合防控体系框架 [7]。

4 总结和展望

“三化六防”的理念措施，是随着我们实际情况不断发展和变化的。从整改建设的角度：建设模式从“局部整改外挂式”，走向“深度融合体系化”；从业务流程的角度，更多地需要考虑业务全流程保障要求，从体系化角度去进行安全规划；从工程实现的角度，将安全需求分步实施，逐步建成面向未来的安全体系；从工作机制的角度，前、中、后三个阶段深入融合形成闭环体系。

对现有防控体系的用户，想要达到“三化六防”的要求还面临不小的挑战，对原有的防护框架进行变革，必定会大大增加企业运行的成本，在新起点、新目标的要求下，网络安全和信息化建设需贯彻“三化六防”理念措施，即未来要具备更强的网络安全攻防能力、预警分析决策能力、风险应对能力，更全面的管控以及更有效的安全运营能力。

参考文献：

[1] 公安部 .《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》公安网〔2020〕1960 号 [EB/OL].http://www.djbh.net/webdev/web/PolicyStandardsAction.do?p=getGlgf&id=8a81825674296d1301749054f4380020,2020-09-15.

[2] 郭启全 . 网络安全法网与网络安全等级保护制度培训教程 :2018 版 [M]. 北京 : 电子工业出版社 ,2018.

[3] 黄一玲 . 中国信息安全观点 .“十四五”网络安全迎来新发展阶段 , 六大视角剖析变革要素 [DB/OL].https://www.secrss.com/articles/32128,2021-06-24.

[4] 国家市场监督管理总局 , 国家标准化管理委员会 . GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》[S].2019-12-01.

[5] 国家市场监督管理总局 , 国家标准化管理委员会 . GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》[S].2019-12-01.

[6] 中国军网 . 网络战专题 [EB/OL].http://www.81.cn/jskj/node_62218.htm,2022-08-15.

[7] 极客元素网 , 等保关保双制度下 , 大型政企如何实现“三化六防”? [DB/OL].https://www.geekmeta.com/article/2298471.html,2020-09-07.