DOI 10.15302/J-SSCAE-2021.02.001

网络空间战略预警体系的建设思考

庄洪林，姚乐，汪生，顾嘉祥，吴晔，解凯

（信息系统安全技术重点实验室，北京 100191）

摘要：网络空间战略预警体系指为早期发现、跟踪、识别、报知来袭的重大战略攻击或烈性病毒传播破坏而建立的警告体系，是国家安全防御体系的重要组成部分；实施网络强国战略需要高度重视网络空间战略预警体系建设。本文分析了网络空间战略预警的主要特点和基本要求，研究了安全漏洞预警、安全威胁预警、入侵攻击预警、异常行为预警等主要预警样式，梳理了国内外网络空间战略预警监测体系的建设情况。研究认为，应重点抓好网络空间测绘系统、漏洞收集预警平台、威胁情报感知推送系统、安全监控综合预警系统等方面的建设工程。研究建议，强化高层统筹协调，注重多源数据融合，设立专业预警机构，开展经常性安全评估， 实行威胁预警分级机制，以此精准保障网络空间战略预警体系建设。

关键词：网络空间安全；战略预警；态势感知；体系建设

中图分类号：TP393　　**文献标识码：**A

Construction of Strategic Early-Warning System in Cyberspace

Zhuang Honglin, Yao Le, Wang Sheng, Gu Jiaxiang, Wu Ye, Xie Kai

(National Key Laboratory of Science and Technology on Information System Security, Beijing 100191, China)

Abstract: Cyberspace strategic early-warning is a monitoring and warning system that is established by a country or group for early detection, tracking, identification, and notification of incoming major cyber attacks or the spreading destruction of powerful viruses. It's an important component of a national security defense system. The implementation of the national cyber development strategy in China requires high attentions to the construction of a cyberspace strategic early-warning system. This study analyzes the major characteristics and basic requirements of strategic early-warning in cyberspace, and studies four major warning styles: security vulnerabilities, security threats, intrusion attacks, and abnormal behaviors warning. It also emphasizes four key projects, namely cyberspace surveying and mapping system, vulnerability collection and early-warning platform, threat intelligence perception and push system, as well as security monitoring and comprehensive early-warning system, after summarizing the construction of strategic early-warning and monitoring systems in cyberspace in China and abroad. To promote the strategic early-warning system in cyberspace, we propose several countermeasures and suggestions, including strengthening high-level coordination, focusing on multi-source data integration, establishing professional early-warning agencies, conducting regular security assessments, and implementing threat and early-warning grading mechanisms.

Keywords: cyberspace security; strategic early warning; situation awareness; system construction

收稿日期：2021-02-05；**修回日期：**2021-03-07

通讯作者：庄洪林，信息系统安全技术重点实验室研究员，研究方向为网络空间安全；E-mail: zhlxsjl@163.com

资助项目：中国工程院咨询项目“网络强国”(2020-ZD-14)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

战略预警指国家为防御突然袭击，运用预警技术及早发现并监视敌对势力战略进攻性武器活动态势的综合性警戒手段，是国家安全的重要保障。当前，网络空间已成为与陆、海、空、天并列的全球第五大空间，是经济社会发展的新支柱、国家安全的新领域。强化网络空间态势感知，提升战略预警能力，确保信息网络疆域安全，是国家安全面临的新型重大课题。

目前，有关网络空间安全预警研究的学术成果主要有：基于入侵事件统计规律的网络安全预警方法[1]、基于决策需求的网络安全战略情报保障能力[2]、基于数据融合的网络安全态势感知技术[3]等。这些研究成果从不同侧面就网络空间态势感知和安全预警建设进行了有益探索。美国基于网络大数据建立了网络空间战略预警体系，通过监控全球网络通信数据、获取国内各大企业服务器数据、共享部门与各盟国间的数据等手段获取情报信息，实现网络安全预警与响应的全系统联动[4]。

为应对日益复杂的网络空间安全形势，有效抵御国家级的大规模网络攻击，我国应高度重视网络空间战略预警体系能力建设，完善网络空间预警机制。本文在理论分析、现状研判的基础上，针对网络资产掌握不全面、安全监测数据难共享、网络攻击取证难等问题，提出了网络空间战略预警体系应建设的重点内容和对策建议。

二、网络空间战略预警的概念、特点及运用价值

（一）网络空间战略预警的基本概念

按照传统定义，战略预警指为早期发现、跟踪、识别来袭的远程弹道导弹、战略轰炸机、巡航导弹等战略武器并及时发出警报所采取的措施。其任务是：尽早探明来袭目标及其各种参数，处理所获信息，对来袭目标进行跟踪、识别，为军事决策、战略武器运用、民防准备等提供实时信息[5]。

网络空间是有别于陆、海、空、天等物理空间的虚拟空间，网络攻击瞬时生效、裂变性强，网络防御的重点是国家级黑客的重大网络攻击、烈性病毒传播破坏。借鉴战略预警的传统定义，网络空间战略预警指一个国家或集团为早期发现、跟踪、识别、报知来袭的重大网络攻击或烈性病毒传播破坏而建立的监测告警体系[6]，是国家防御体系的重要组成部分。

（二）网络空间战略预警的特点

相比物理空间对抗，网络空间攻防有其自身的独特机理，由此带来网络空间战略预警与传统物理空间在国家战略预警方面的显著区别。惟有深刻认识网络空间对抗的机理特点，才能更有效地开展战略预警工作。

1. 预警的职责主体为政府

物理空间的边界明确，对外防卫主要表现为陆防、海防、空防、天防，其中来自空、天的战略武器威胁较大[7]，相应战略预警的职责主要由国防专业力量承担。互联网、电信网是网络空间的主体，相应管理主要由政府部门负责。按照“谁主管，谁负责”的原则，网络空间战略预警的职责主体应是政府。

2. 预警防范对象更广

网络攻击既可以来自外部实施，也可以从内部发起；既可能是国家行为，也可能是非法组织或个人行为。物理空间的防范对象主要为敌对国家军队，而网络空间防范的对象既包括国家级高级可持续威胁攻击（APT）组织和恐怖势力，也包括民间黑客组织和内部人员。因此，网络空间战略预警防范的对象范围更广、更复杂。

3. 预警时间更加短促

网络攻击会对目标直接发起攻击并瞬时生效，网络的互通性、病毒的裂变传播性不仅会使受攻击网络出现“一机中招、多机感染、区域瘫痪”的局面，还会跨网迅速扩散并影响其他网络。与传统物理空间战略攻击通常因诱发因素出现战争动向相比，网络空间的攻击门槛低，攻击时间随机且短促，随时都有可能遭受敌对势力和黑客攻击，因此提前预警的迫切性凸显。

4. 预警目标动态性强

网络信息技术不断发展，针对网络特性变化、技术设施更新，网络空间攻击手段不断调整升级，攻防手段在博弈中互相促进、竞争发展，呈现出此消彼长、互促互进的态势。就某种具体的网络攻击手段而言，攻击效果也是动态变化的，对战略性评

估构成了挑战。

5. 战略性判定与防御对象属性相关

远程弹道导弹、战略轰炸机、巡航导弹等实体空间武器的战略性很容易界定，国际上也有一致认可。网络攻击武器针对性强，攻击效果与受攻击方的网络结构、属性以及所采用的软硬件系统、防范机制等密切相关，不易判定。因此，衡量一种网络攻击手段是否具有战略性，需结合被攻击对象的网络属性特征；只有匹配并可达成战略性威胁的网络攻击手段，才应列为重点预警对象。

（三）网络空间战略预警的运用价值

网络空间对抗具有技术性强、目标多元、要素复杂、时间敏感、地域模糊、数据量大等特点，建设具有全面掌握网络软硬件资产情况、深度挖掘信息系统安全漏洞、广泛获取网络攻击手段与行为特征、实时感知网络攻击威胁、有效监测并汇聚各种异常行为、分析发现安全事件内在关系、综合研判网络安全发展态势等核心能力的网络空间战略预警体系，对于网络防御行动的科学决策、赢得主动，推进网络治理能力现代化具有重要的战略意义。

第一，网络空间战略预警是快速、高效处置重大网络安全事件的重要基础。构建网络资产基础信息库、挖掘掌握信息系统安全漏洞是网络空间战略预警的基础环节。地图是人们认知理解环境的重要工具，虚拟的网络空间同样需要由详实信息构成、完整描述各要素状态关系的“网络地图”，即网络资产基础信息库；对于重要大型网络，加强网络软硬件资产的安全管理至关重要。部署网络空间资产探测系统，掌握网络体系架构、重要节点、关键设备、重点保护对象，发现“风险资产”，是实施网络防御行动的基础。网络攻防在很大程度上表现为漏洞利用与修补在时间窗口上的博弈，基于已构建的网络资产基础信息库，可在发现新漏洞的第一时间从信息库中快速搜寻出受漏洞影响的网络设备及地址，从而为开展积极防御行动、及时进行漏洞修复提供精准的目标指向。

第二，网络空间战略预警是掌握网络空间防御战略主动的重要保障。掌握网络威胁行为特征，构建威胁情报支持平台，可为实施安全预警提供可靠的情报保障。目前，世界上约有数十万名黑客，对于国家层级的黑客群体，防御方需要时刻感知其攻击的技术手段、行为特征和所威胁的系统，掌握其攻击代码并监测发展变化，评估己方网络面临的潜在危害，从而实施有效应对。即使是发生在其他地方的网络攻击，掌握其攻击代码和行为特征，对于监测和预警针对己方网络的威胁、掌握网络空间防御战略主动，同样具有重要意义。

第三，网络空间战略预警是综合把握网络空间安全态势的重要手段。传统的单一入侵检测系统已经过时，单机杀毒软件容易失效。构建以大数据、云技术为支撑，注重多源数据融合和情报共享，通过各类系统的综合集成，形成全域覆盖、上下贯通的完整体系，构建一体化、分布式结构的安全监控综合预警系统，有助于提高对异常行为的获知能力，发现潜在未知威胁，精确定位攻击源头，预判安全事件演变趋势。

三、网络空间战略预警的基本要求和应用样式

（一）网络空间战略预警的基本要求

网络空间战略预警应具有发现、跟踪、识别网络空间战略破坏的能力以及分析判断和网络反制的溯源能力[8]。为此，网络空间战略预警体系需要具备以下基本能力：①全面性，在难以判断危害严重程度的情况下，按照“不漏情”的原则对危害网络空间安全的行为进行预警；②预控性，鉴于网络空间预警时间短促，有必要将网络空间战略预警关口前移，平时常态化开展网络空间安全或战略危机的分析预测，实施早期控制；③诊断性，在网络系统建设和管理过程中，对可能存在的网络安全问题进行强化测试和诊断，记录网络软硬件及其状态，据此分析判断各类网络攻击手段的潜在危害；④动态性，密切跟踪网络新技术发展、新问题发现、环境因素的新变化，及时调整我国网络建设的发展思路、应对全球网络攻击手段变化，同时持续加强分析判断模型、应对措施方法的更新升级；⑤规范性，运用系统性的计划策略和理性分析方法，开展针对网络危害战略性判断、应对措施与方法的程序化决策。

（二）网络空间战略预警的应用样式

1. 安全漏洞预警

安全漏洞预警属于早期预警，主要是通过主动挖掘和分析重要网络设备、操作系统、应用软件、应用服务系统（如域名服务系统、电子邮件系统）等存在的安全漏洞缺陷，及时发现系统中存在的后门、设计缺陷以及设备与系统管理漏洞，尽早开展封堵处理，防止被恶意利用；主要针对国际上尚未公布的安全漏洞进行预警。

2. 安全威胁预警

安全威胁预警属于中期预警，主要是通过部署的网络空间资产探测系统、网络空间威胁情报感知系统，发现“风险资产”，实时跟踪监测重要网络被控、全球僵尸网络构建、蠕虫病毒传播、黑客组织攻击活动、已公开的安全漏洞、网络攻击最新技术手段等情况，预测潜在的网络破坏性攻击行为对网络系统安全带来的影响范围、危害程度、持续时间等；按照规定和程序，及时通报相关威胁，尽快采取应对措施；主要针对已经在其他地方出现，但尚未涉及到所防护网络的威胁源。

3. 入侵攻击预警

入侵攻击预警属于临近预警，主要是通过在网络信道出入口、重要服务器、重要应用系统等关键部位布设网络入侵检测系统、行为审计系统，实时监测网络攻击者对网络的渗透、重要数据访问等异常行为；发现后实时报警、响应，通过其他防护系统自动进行行为中止或由安全防护人员迅速处置，阻止大规模入侵、破坏行为的发生，防止事态扩大；主要针对已经接触到所防护网络的攻击行为。

4. 异常行为预警

异常行为预警属于对内预警，主要是通过监测、审计重要内部网络的用户操作和网络行为，及时发现违规操作、蓄意破坏、病毒传播等直接危害网络安全的异常情况，准确追踪定位威胁源头；主要对发生在内部网络中的异常行为或攻击企图进行预警。

四、网络空间战略预警监测体系的发展现状

（一）国外网络空间预警监测建设情况

信息基础设施发达的国家和地区高度重视网络空间安全战略预警能力建设。以美国为例，代表性做法如下 [4]。

一是打造全球网络通信数据监控能力。一方面，美国依托其全球信息枢纽的优势地位，在重要数据交换节点上大规模搜集基础性数据；另一方面，采取改造监控海底光缆等手段，将网络监测范围覆盖至美国境外地区；已将互联网骨干网中 50% 以上的流量纳入到监测范围。

二是政府相关部门加大对大型网络运营商、互联网服务商监测数据的利用力度。斯普林特公司、电话电报公司、威瑞森通信公司等顶级骨干网运营商，微软公司、谷歌公司、脸谱公司、苹果公司等互联网服务提供商，都是情报机构的合作对象；对相应的流量数据、网络行为数据等进行大数据关联分析，找出潜在威胁。

三是广泛开展深度的信息合作与数据共享。国土安全部、国防部、司法部强调对各自掌握的情报信息实施互联互通，建立行动性、预警性情报的“一知皆知”通报制度，实现网络安全预警及响应的全系统联动。同时，美国与英国、法国、德国等设立了基础性的互联网数据信息共享机制。

网络空间预警监测系统，如“爱因斯坦计划”入侵防御项目，旨在支持政府机构应对网络空间安全威胁，提供入侵检测、入侵防御、取证分析、信息共享等能力。“爱因斯坦计划”由国家统筹规划、统一部署，监视政府各部门的网络出入口流量；一旦遭受网络攻击，监测系统将自动向国土安全部下属的美国计算机应急响应小组（US-CERT）报警，安全专家将实时纵览跨机构的安全事件并采取应急处置措施 [9,10]。

（二）我国网络空间战略预警监测体系建设情况

1. 法律法规层面

在网络监测预警与应急处置方面，《中华人民共和国网络安全法》明确了国家和省级相关政府职能部门的职责，为国家网络空间安全预警、安全事件处置提供了法律保障。该法规主要强调，国家网络安全和信息化部门应注重统筹协调，加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息；建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，

定期组织演练。负责关键信息基础设施安全保护工作的部门，应建立健全本行业、本领域的网络安全监测预警和信息通报制度，按照规定报送网络安全监测预警信息；制定本行业、本领域的网络安全事件应急预案，定期组织演练。在网络安全事件发生风险可能增大时，省级以上人民政府有关部门应按照规定的权限和程序，根据网络安全风险的特点和可能造成的危害采取措施。

2. 技术层面

许多网络安全公司已建有较为成熟的网络威胁感知分析平台，主要采取互联网在线探测感知、重要网络枢纽探测感知两种方式，广泛收集互联网设备信息、出入口流量、安防系统运行数据，再经过大数据和人工智能分析，感知网络基础设施、关键业务网络的威胁，在一定程度上实现了针对网络攻击的早期发现、入侵途径回溯、攻击源定位。国内外一些网络安全公司建有专门的网络空间测绘平台、漏洞收集分析平台并在互联网上开放服务，可为网络空间战略预警、安全事件快速处置提供数据支撑。

3. 当前面临的主要问题

①网络资产掌握不够，缺乏全面的网络资产基础数据库，政府部门、重要行业的单位企业对自身网络资产信息掌握不够，在态势分析、应急响应处置方面缺少资产数据支撑。②安全监测数据不能共享，国家关口数据、城市区域数据、行业内网数据不能汇聚，各单位之间缺乏监测数据、威胁情报感知数据的共享机制，无法全面开展网络攻击事件的综合性关联分析。③网络攻击行为的取证难度大，有的单位在遭受网络攻击后，拒绝提供取证数据，甚至擅自删除日志，影响了网络攻击行为的溯源与追踪，降低了国家网络空间战略预警的实际效果。

五、网络空间战略预警体系的重点建设内容

（一）网络空间测绘系统

网络空间测绘系统是网络空间战略预警体系建设的基础。只有全面掌握自身网络的软硬件资产情况，才能在网络防御行动中掌控全局、争取主动。开展网络空间测绘，要以大规模网络空间软硬件资产探测为先导，以主动感知、大数据挖掘分析、知识学习推理、可视化展示等关键技术为支撑，强化网络空间软硬件资产基础库构建与数据深度挖掘分析，实现网络空间地图的多层级直观展示。

（二）漏洞收集预警平台

漏洞收集预警平台是预警体系早期预警的主要手段。漏洞信息主要通过自主挖掘、国内外相关机构公开的漏洞库、社会人员提交等方式获得。截至 2021 年 3 月 5 日，全球公开漏洞披露平台（CVE）包含了约 1.49×10^5 个公开漏洞 [11]，我国国家信息安全漏洞库（CNNVD）包含了约 1.59×10^5 个公开漏洞 [12]。这些漏洞数据库提供了漏洞名称、编号、类型、来源、威胁类型、危害等级、修复补丁、漏洞影响的具体设备、软件版本等基本信息。但多样化的漏洞信息来源存在数据格式不统一、非结构化等问题，需要专业人员开展进一步的融合分析、验证、整理，统一结构化设计，构建兼容不同数据格式的漏洞预警信息库，并根据需要进行信息发布和定向推送。此外，还需注意漏洞信息库中关键字段与软硬件资产库的适配性设计，为网络空间态势感知、快速进行威胁预警提供数据支撑。

（三）威胁情报感知推送系统

威胁情报感知推送系统是预警体系中期预警的主要手段，分为威胁情报感知信息库、威胁情报分析推送系统两部分。威胁情报感知信息库主要通过人工收集、自动采样、网络平台获取、公开数据库查询等方式获取信息，信息经分析整理后入库；相关内容包括：互联网中曾发起过攻击行为的地址、黑客使用过的设备和域名、各种病毒木马等恶意代码样本、漏洞安全威胁、黑客行为特征与手段、危险超链地址、恶意软件黑名单、某种攻击可能威胁到的设备和系统等信息。威胁情报分析推送系统主要针对特定威胁、特定防护目标、新发布漏洞，通过智能化数据挖掘与匹配算法，发现重要目标潜在的安全威胁，智能化、自动化、定向快速推送相关预警情报信息。

（四）安全监控综合预警系统

安全监控综合预警系统是预警体系临近预警的主要手段，分为流量监测分析系统、网络入侵取证与行为审计系统等。流量监测分析系统布设在网络干线节点、各接入网出入口等位置，主要实现干线

数据采集、异常网络流量分析检测、攻击代码检测捕获、安全事件融合分析、安全态势综合显示、阶段性网络数据存储回访等功能。网络入侵取证与行为审计系统部署在重要网络系统和关键服务节点，主要进行网络攻击的快速准确定位。通过相关系统的综合集成，构建一体化、分布式结构的安全监控综合预警系统。

六、对策建议

（一）强化顶层设计，加强统筹协调

网络空间安全事关国家安全大局，需要做好顶层设计，多部门统筹并协调开展工作。战略预警作为网络安全的首要环节和常态化工作，应整体统筹、分工推进。建议由国家相关主管部门集中统一领导，统筹网络空间战略预警规划、系统建设、安全风险评估、重大事件应急响应等工作；各级政府部门、相关行业开展预警监测和应急响应工作，依据职能分工，发挥各自优势，协作开展。

（二）注重多源数据融合和情报共享，打牢国家网络空间战略预警基础

建立和完善国家级安全防御预警监测体系，全面汇聚政府部门、事关国计民生重要信息系统的互联网出入口数据、重要单位的威胁情报数据。基于分布式前端数据收集、集中化后端数据分析模式，对多源数据进行关联分析处理，及时分发经过汇聚处理的情报信息，提升国家对网络潜在异常行为的获知能力、对网络攻击事件的检测与协同防御能力；及时发出安全预警并采取相应对策，必要时跟踪溯源，对攻击者进行定位，为有效应对网络攻击提供支撑。

（三）加强多方专业力量参与，健全网络空间战略预警力量体系

我国已在安全漏洞、病毒木马、黑客攻击等方面建立了较为顺畅的交流机制，具备了较强的网络安全威胁早期预警和安全事件快速处置能力[13]。建议进一步健全由国家、行业和单位三级力量构成的网络空间战略预警力量体系。在国家相关部门的统筹协调下，积极引导高等院校、科研院所等有能力的单位参与，担负操作系统软件、重要信息系统软硬件产品的漏洞分析任务，及时发现并排除各种预置后门和设计缺陷。重要网络应用行业的网络安全防护专业力量，负责本行业专用软件和重要应用软件的漏洞分析检测，查找信息系统研制和集成过程中存在的安全漏洞；制定量化评定检查标准，对本行业内部网络进行经常性安全风险评估检查。各单位网络安全防护力量，针对所属保障范围内的网络信息系统，对本级和下级单位的内部网络进行安全风险评估检查，查找安全漏洞并提出改进意见。

（四）开展经常性安全评估，促进隐患早诊断、早发现

网络安全是相对的、动态的，需要在网络应用过程中不断查找和发现问题，力求提前防范，这是实现网络安全早期预警最重要的内容。建议在行业内部强化经常性安全评估，政府相关部门组织网络安全保障演练，及时查找种隐患，尽早提出应对措施，促进网络安全防护能力的快速、持续提升。

（五）实行威胁预警分级机制，规范并细化配套应对措施

美国、俄罗斯等国家对恐怖威胁的预警一般分为三级，如美国为公告预警、升级预警、紧急预警，俄罗斯则以蓝、黄、红 3 种颜色，从低到高进行级别划分[14]。我国网络空间战略预警可参考国际恐怖威胁预警的通常做法，进行蓝、黄、红分级，并根据不同等级提出相应的应对措施。蓝色预警主要针对重大漏洞发现、境外发生重大网络攻击，有可能对我国网络安全造成较大危害的情况；黄色预警主要针对危害性大的病毒蠕虫传播、黑客组织对我国实施的较大规模网络攻击，将造成重大危害的情况；红色预警主要针对敌对势力、恐怖组织对我国网络基础设施、事关国计民生重要信息系统实施的大规模扰乱瘫痪攻击，预期后果特别严重的情况。

（六）发挥互联网企业作用，建设网络空间战略预警队伍

增强互联网企业在网络安全领域的使命感和责任感，共同促进互联网产业的持续健康发展，确保企业稳健成长，这既是企业奋斗的目标，也是国家

发展的需要。网络空间安全战略预警宜发挥互联网企业在网络空间测绘、漏洞挖掘、网络安全监测、大数据分析等方面的技术、产品、数据、人才优势，建成覆盖事关国计民生重要网络、全面应对网络空间各种重大威胁、快速处置重大安全事件的网络空间安全战略保障队伍。

参考文献

[1] 张峰, 秦志光, 刘锦德. 基于入侵事件预测的网络安全预警方法 [J]. 计算机科学, 2004, 31(11): 77–79, 129.
Zhang F, Qin Z G, Liu J D. Intrusion event based early warning method for network security [J]. Computer Science, 2004, 31(11): 77–79, 129.

[2] 陈明, 王乔保, 汤文峤. 网络空间安全战略情报保障能力研究 [J]. 情报杂志, 2020, 39(4): 127–131.
Chen M, Wang Q B, Tang W Q. The capability of strategic intelligence supporting for cyberspace security [J]. Journal of Intelligence, 2020, 39(4): 127–131.

[3] 龚俭, 臧小东, 苏琪, 等. 网络安全态势感知综述 [J]. 软件学报, 2017, 28(4): 1010–1026.
Gong J, Zang X D, Su Q, et al. Survey of network security situation awareness [J]. Journal of Software, 2017, 28(4): 1010–1026.

[4] 吴彤. 境外信息网络监控形势与挑战 [J]. 国防科技, 2016, 37(3): 40–43.
Wu T. Situation and challenges of overseas information network monitoring [J]. National Defense Technology, 2016, 37(3): 40–43.

[5] 李鸿飞, 田康生, 金宏斌. 浅析战略预警空天目标与识别 [J]. 飞航导弹, 2015 (6): 30–33.
Li H F, Tian K S, Jin H B. Analysis on strategic early warning aerospace target and identification [J]. Aerodynamic Missile Journal, 2015 (6): 30–33.

[6] 宣蕾, 苏金树, 苗青, 等. 网络安全战略预警系统研究 [J]. 通信技术, 2001 (7): 90–92.
Xuan L, Su J S, Miao Q, et al. Study on network security strategic indication/warning system [J]. Communications Technology, 2001 (7): 90–92.

[7] 刘凤增, 肖兵, 刘捷, 等. 美国战略预警体系发展探析 [J]. 飞航导弹, 2019 (3): 65–69.
Liu F Z, Xiao B, Liu J, et al. Analysis on the development of American strategic early warning system [J]. Aerodynamic Missile Journal, 2019 (3): 65–69.

[8] 冯伟, 梅越. 大数据时代, 数据主权主沉浮 [J]. 信息安全与通信保密, 2015 (6): 49–51.
Feng W, Mei Y. In the era of big data, data sovereignty rises and falls [J]. Information Security and Communications Privacy, 2015 (6): 49–51.

[9] 俞飞. “爱因斯坦计划”升级美国网络安全 [J]. 保密工作, 2013 (8): 54–55.
Yu F. “Einstein plan” upgrades American cyber security [J]. Confidential Work, 2013 (8): 54–55.

[10] 赵阳光, 黄海波. 美国“爱因斯坦计划”研究 [J]. 信息安全研究, 2020, 6(11): 1013–1016.
Zhao Y G, Huang H B. American “Einstein plan” research [J]. Journal of Information Security Research, 2020, 6(11): 1013–1016.

[11] Common Vulnerabilities & Exposures Numbering Authorities. Common vulnerabilities and exposures [EB/OL]. (2021-03-05) [2021-03-06]. http://cve.mitre.org/cve/.

[12] 国家信息安全漏洞库. 漏洞信息 [EB/OL]. (2021-03-05) [2021-03-06]. http://www.cnnvd.org.cn/web/vulnerability/querylist.tag.
China National Vulnerability Database of Information Security. Vulnerability information [EB/OL]. (2021-03-05) [2021-03-06]. http://www.cnnvd.org.cn/web/vulnerability/querylist.tag.

[13] 周勇林. 计算机应急响应与我国互联网应急处理体系 [J]. 世界电信, 2004 (3): 33–38.
Zhou Y L. Computer network emergency response and internet emergency coordination system in China [J]. World Telecommunications, 2004 (3): 33–38.

[14] 戴艳梅. 俄罗斯反恐机制研究 [J]. 俄罗斯东欧中亚研究, 2012 (5): 31–38, 95–96.
Dai Y M. Research on Russian anti-terrorism mechanism [J]. Russian, Central Asian & East European Studies, 2012 (5): 31–38, 95–96.