中国指挥与控制学会
CHINESE INSTITUTE OF COMMAND AND CONTROL

中国指挥控制大会
CHINESE CONFERENCE ON COMMAND AND CONTROL

第二届中国指挥控制大会论文集

——网络时代的公共安全与应急救援

中国指挥与控制学会 编

国防工业出版社
National Defense Industry Press

第二届中国指挥控制大会论文集
——网络时代的公共安全与应急救援

中国指挥与控制学会　编

国防工业出版社
·北京·

图书在版编目（CIP）数据

第二届中国指挥控制大会论文集/中国指挥与控制学会编. —北京：国防工业出版社，2014.7

ISBN 978-7-118-09653-8

Ⅰ. ①第… Ⅱ. ①中… Ⅲ. ①指挥控制系统－学术会议－中国－文集 Ⅳ. ①E072-53

中国版本图书馆 CIP 数据核字（2014）第 162582 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号 邮政编码 100048）

北京京华虎彩印刷有限公司印刷

新华书店经售

*

开本 880×1230 1/16 **印张** 59¼ **字数** 2150 千字

2014 年 7 月第 1 版第 1 次印刷 **印数** 1—1300 册 **定价** 298.00 元（全二册）

前　言

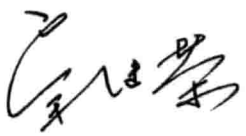
为了贯彻落实党的十八大报告对加强海洋、太空、网络空间安全的明确要求，以及十八届三中全会进一步对维护国家安全、推进信息时代的国防和军队现代化建设、推动军民融合深度发展的要求，加快推进指挥控制科学技术在公共安全、反恐维稳、应急救援等非战争军事行动能力建设中的作用，展示和交流近年来指挥控制技术在云计算、物联网以及大数据环境下公共安全、应急救援和军队现代化建设中的研究成果，进一步提升国家在指挥与控制科学技术成果推广应用中的能力和水平，促进指挥控制技术领域军民融合，为指挥与控制科学技术进步和产业创新提供一个良好的交流平台，中国指挥与控制学会于 2014 年 8 月在北京举行“第二届中国指挥控制大会”。

“中国指挥控制大会”是国内指挥控制领域集高端学术交流、先进产品展示、产学研协同创新为一体的全国性、综合性大会，是推动信息时代我国指挥控制科技产业创新发展的重要力量。自第二届中国指挥控制大会征文以来，受到指挥控制领域学者们的广泛关注，我们深切地感受到广大学者对指挥控制领域的热情，为学科进步贡献自己一份力量的殷切希望，以及对中国指挥控制大会的支持。论文集的出版，展现了我国指挥控制技术领域科研工作者近年来的最新成果与发现。其中不仅有从事该领域多年的专家对学科领域发展的深刻见地和丰富经验的总结，还有大批青年学者对学科领域的创新思维、大胆设想和独到的见解。他们将科研实践、思考、探索与总结中的成败得失，将生产研发中面对大量实际问题所得的宝贵经验撰写成文，为推动指挥控制学科技术领域的发展、开阔技术视野、拓展研究思路提供了良好的借鉴。

论文集作为指控大会成果展示的一部分，努力做到让每一位对指挥控制技术领域有期许、有兴趣的同行可以得到行业内最新的研究成果。为保证会议质量，充分反映当前指挥控制领域学科发展焦点，有效提升会议学术交流水平，大会组委会分专题建立审稿专家库，对“发展中的指挥与控制”、“网络时代的公共安全”、“大数据时代的灾害防护与应急救援”三个专题的论文进行评审，选出 219 篇论文汇编成“发展中的指挥与控制”与“网络时代的公共安全与应急救援”上下两册，构成“第二届中国指挥控制大会论文集”出版发行，献礼本次盛会。

“路漫漫其修远兮，吾将上下而求索”，值此论文集出版之际，对所有关心与支持本届中国指挥控制大会的单位、领导、专家和学者表示衷心的感谢。同时祝愿同行们在指挥控制技术领域的探索道路上取得更大的成果，祝愿中国指挥与控制学会的明天更加辉煌。

中国指挥与控制学会　秘书长



上册目录

专题一 发展中的指挥与控制

综述

指挥控制系统研究

火力与控制系统研究

系统建模与仿真研究

信息处理技术研究

通信网络技术研究

下册目录

专题二　网络时代的公共安全

专题三　大数据时代的灾害防护与应急救援

专题二

网络时代的公共安全

指挥信息系统面临的网络安全威胁及对策

杨　涛[1]，谢爱华[1]，段　娟[2]
（1．77200部队，云南昆明　650032；2．云南省武警总队，云南昆明　650000）

摘　要：指挥信息系统已经成为体系作战能力生成的基础支撑，在网络安全威胁环境下如何应对网络攻击威胁，提高网络防御能力，确保系统效能可靠发挥，已经成为我军信息化、网络化进程中需重点关注的时代课题。本文分析了网络威胁的特点，阐述了指挥信息系统面临的安全挑战，提出了相应对策措施。

关键词：指挥信息系统；网络安全；栅格化；一体化
中图分类号：E25　　**文献标识码：**A

The Threat To The Network Security And Corresponding Strategies in The Command Information System

YANG Tao，XIE Ai-hua，DUAN Juan
(1．77200 Troop of PLA, Kunming Yunnan　650032,China；2．Yunnan Provincial Armed Police Corps , Kunming Yunnan　650221,China)

Abstract: Command Information System has become the basis for the systematic combat capability to generate support. It has become the army of information and network processes need to focus on the topic of the times that, how to deal with the threat of cyber attacks in the network security threat environment, improve network defense capabilities, ensure reliable system performance to play. This paper analyzes the characteristics of network threats, describes the security challenges facing the command information system, put forward the corresponding solutions and methods.

Key words: command information system；network security；grid；integration

0　引言

指挥信息系统[1]融合了指挥控制、情报侦察、预警探测、网电对抗、火力打击、后装保障等诸要素，是军队的神经中枢，也是敌对双方破袭的重点。网络安全正是国家信息化水平发展到一定阶段而必然出现，并将对基于信息系统的体系作战能力构成极大挑战的课题。积极应对网络安全威胁，提高指挥信息系统网络防御能力，确保系统效能可靠发挥，围绕信息系统展开针对性的安全防护研究和训练，已经成为系统建设和运用中不容回避的环节。

1　网络安全威胁的特点

1.1　在样式上表现为非对称性，易攻难守

网络安全威胁[2]以信息网络基础设施、计算机系统等为对象。随着网络攻击技术的不断发展，网络攻击方式不断涌现，隐蔽性和破坏力越来越强。同时网络防御在全方位展开，在传输、存储、系统、应用各环节都会遭受多种攻击，稍有漏洞便被攻击者利用。从交锋回合上看，上百次的进攻，只要有一次成功，就能取得决定性战果；相反，上百次防御，只要有一次失手，就会前功尽弃。

1.2　在时空上表现为全天候、全空域随机作战，攻击源头难以准确定位

网络空间无边界，网络业务在网络空间畅通无阻，组织和个人都能平等的接入网络，不受限制或很少受限制的自由通信。加之网络攻击在网络上以光速传播，瞬间即可完成攻击，而且网络IP地址能够作假，很难判断攻击源真实位置和起止时间。

1.3　在作战形式上表现为开放性、非接触作战

由于信息技术的军民通用性和计算机网络的互联开放性，使得网络攻防力量非常广泛，军队、普通公民都可以介入网络安全威胁。作战对象远隔万里，在电脑前点击鼠标即可达成攻击。通过“僵尸网络”、跳板等攻击手段，攻击者甚至不需要与目标产生任何网络连接和数据交互。

作者简介：杨涛（1977—），男（白），云南大理人，高级工程师，硕士，主要研究领域为计算机网络技术、指挥信息系统、数据网格。E-mail:tsinxin@126.com。

1.4 在目标选取上为以指挥信息系统中心节点为攻击重点

随着数字化网络在军队作战指挥中的普及运用，作战样式由传统的火力战向网络空间延伸，兵不血刃同样能够决定战争的胜负。美军21世纪以来开始推出Suter（舒特）[8]系统，由“高级侦察员”系统、EC-130H信息对抗飞机和RC-135远距离侦察飞机通过NCCT（网络中心协同目标瞄准网络）互联而成，可以监测敌方防空雷达图像，侵入地方防空网络并操纵传感器，控制敌方防空网络。

1.5 在本质上是信息基础设施和专业技术的较量

网络安全威胁是在网络空间以信息技术为基础的有组织的较量，技术的重要性等同于武器和战术，一个算法、一段代码将产生的效应可能可以不亚于原子弹和氢弹。在网络安全威胁背景下，发达国家关乎国计民生的核心技术是永远不会与人共享的。自主创新不仅在经济领域，在军事领域也是至关重要的。

2 网络安全威胁给指挥信息系统带来的挑战

指挥信息系统以信息基础设施为依托，以综合诸兵种要素业务的软件系统为核心，与信息作战、武器平台相链接，与民用信息系统融合，在网络安全威胁中面临多种威胁。

2.1 指挥信息系统位于指挥平台的中心，节点被攻破可能造成全网或部分瘫痪

我军指挥信息系统是一个跨军兵种的广域网络，处于指挥平台的中心位置，以业务信息系统为核心，将各种武器系统、作战要素连接到一起，以简单的、机械的、层次的互连互通，交互层次多，共享能力不强，功能融合度不高。网络安全威胁环境下，信息系统一旦中心被摧毁，全系统将瘫痪，一个节点被摧毁，与节点下连的单元将退出战斗。

2.2 指挥信息系统建设不规范，网络防御整体合力不强，面临各个击破的威胁

目前我军指挥信息系统顶层设计上还有很多不完善的地方，还存在各军兵种各自为战，分头建设的现象。指挥信息系统在功能、数据、技术体制上还没有实现完全融合。由于不同系统采用的技术体制各异、数据库割裂独立难共享、开发和运行环境不同，安全配置要求也不同，甚至有少量冲突，没有深入细致的管理，就会在系统中留下漏洞和弱点，很难形成统一的安全防护策略，容易导致在个别系统和节点率先被攻破，最终各个击破。

2.3 国家和军队信息基础设施相对落后，关键软硬件技术受制于人，信息网络潜藏重大风险

目前与发达国家相比，我国自主产权信息技术和基础设施还有差距，政府和军队还在大量使用国外的计算机、网络、信息设备核心技术，如美国微软的Windows操作系统、Office办公软件，甲骨文Oracle数据库，英特尔、AMD的CPU，Cisco的路由器、交换机，日本的集成电路等。事实证明这些软硬件中存在着各种安全漏洞和安全后门，为我军核心网络和指挥信息系统安全埋下了隐患，因此指挥信息系统的脆弱性将继续存在，要确保网络和系统安全，就必须持续升级防护措施。

2.4 网络攻击技术飞速发展，对指挥信息系统造成的威胁急剧增长

网络攻击手段多种多样，攻击技术发展很快。从病毒破坏、木马渗透到逻辑炸弹引爆，还有恶意代码攻击、非授权访问攻击、非正常使用攻击、缓冲区溢出攻击和拒绝服务攻击等，方法手段五花八门。电磁脉冲弹、次声波武器、激光反卫星武器、高功率微波武器等对信息网络系统能产生致命破坏。近年来，以美国为首的军事强国不断加强新概念、新机理网络武器[6]的研制，包括破坏电子电路的微米/纳米机器人、啃食硅基电子芯片的细菌、网络数字大炮等。美军“舒特”系统已经进入实战运用。

2.5 官兵安全保密意识不强，指挥信息系统使用管理存在受到网络攻击的隐患

我军指挥信息系统虽然与互联网物理隔离，但由于管理措施不到位或安全意识不强，受到网络攻击的可能性不能排除。一是内部管理人员和使用者由于误操作、违规操作，如存储介质的交叉使用，不慎把敌特分子预先开发的网络攻击软件带入内部系统，在关键时刻攻击破坏指挥信息系统。二是信息设备在生产、采购、维修、升级等过程中控制不力，被敌特分子植入破坏程序。三是极少数内部人员可能被腐蚀拉拢、甚至被策反，成为敌人发起网络攻击的代理人。指挥信息系统监管难度大、中间环节多、容易出现疏漏，有可能被利用。

3 对策思考

3.1 积极稳妥推进指挥信息系统栅格化，提升网络抗毁能力

栅格化信息网[3]是下一代指挥信息系统发展的目标和方向。指挥信息系统从单兵单装到作战单元，从

独立器件到复杂系统都能以随遇、多路由、自动连接，形成具有统一指挥、信息充分共享的有机整体，系统能对所有作战资源进行有效管理和动态配置，当一个节点被摧毁，该节点的功能将被其他节点替代，继续维持整个系统的作战功能，提高指挥信息系统的抗毁能力。随着栅格化建设推进，各类指挥机构、传感器、武器系统、保障装备等作战资源将大量接入系统，为指挥信息系统组织运用提供更大的灵活性和系统容量。积极稳妥推进栅格化指挥信息系统建设，同步展开安全防护技术、战术研究，提高系统安全防护能力，系统结构如图 1 所示。

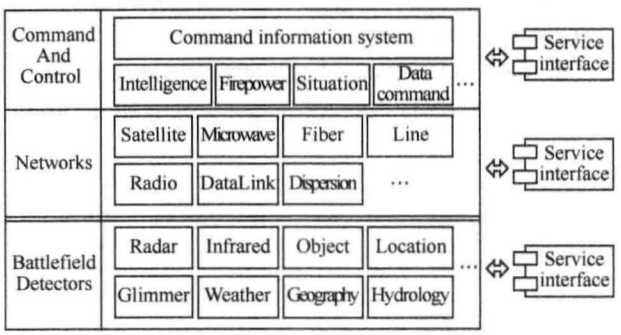


图 1　栅格化指挥信息系统结构示意图

3.2　按照统一的技术标准来推进指挥信息系统一体化建设，打牢系统安全基础

在指挥信息系统的建设中必须严格贯彻落实统一的技术标准，一方面可以为系统互联互通互操作提供技术支撑和标准支持，适用于指挥信息系统建设的总体设计、需求论证、组织实施、质量监督、系统验收以及升级改造全过程。通过遵循统一的标准体系，实现不同层次、不同类型的指挥信息系统作战需求的规范化描述，基础数据的统一表示，信息服务的可发现、可访问、可信任。避免出现因不同应用需求和技术体制造成的“烟囱”林立局面。另一方面通过指挥信息系统的标准化建设，可以提升系统整体的安全防护能力。且不说一些不成熟的技术没有经过长期的检验，存在较大的安全漏洞；一些成熟的技术，由于技术人员不熟悉，也会在配置上使用上带来安全风险。只有严格贯彻落实统一标准，遵循统一的国军标、技术参考模型和互操作性标准，才能从技术体系上打牢系统安全基础。要把技术标准体系推广应用纳入指挥信息系统建设的全局，甚至要先行一步，只有在标准上紧跟信息技术发展，不断更新标准，提高科学性和准确性，从而能够更好的指导系统建设。

3.3　强化指挥信息系统安全防护管理措施，完善技术防护体系

在强化指挥信息系统安全防护管理措施[7]方面，要把好病毒、木马、蠕虫等破坏程序的入口关，对普通使用人员的操作行为进行技术监督。一是从提高使用人员的安全意识和信息化素养入手，防止误操作、违规操作，防范违法行为。二要贯彻落实信息安全保密规章制度。严格遵守保密等级来落实安全防护系统建设。指挥信息系统终端严格安装保密管理、主机监控等系统，禁用普通终端读写设备，完善审查、过失追踪程序。在技术防护手段上，一要继续严格执行信道加密、接入控制、边界防护、外部信息交换加密、内网防护与内部信息加密防线，升级设备功能。二要提高网络防病毒系统的工作效率。必须及时更新病毒库，快速处理控制台报警事件，不留监控死角，建立科学的病毒事件应急处理机制和响应流程。三要建设多级容灾备份数据中心。对指挥信息系统的数据管理模式进行改造，剥离具体业务分系统实行数据中心集中统管。利用 SAN、NAS、DAS 存储技术，配套建立加密以及基于应用、角色、用户、IP、主机标识访问控制技术手段，动态备份系统数据，提高数据安全防护能力。

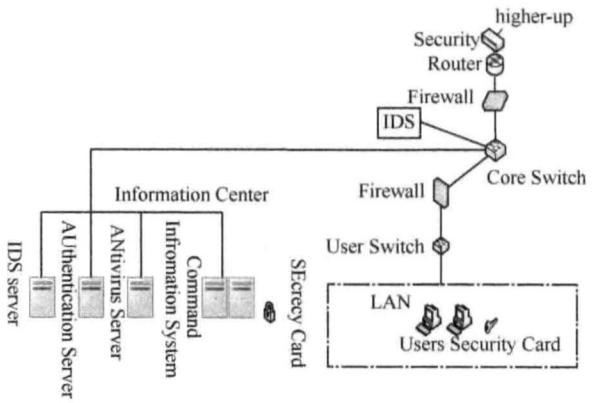


图 2　指挥信息系统安全防护体系示意图

3.4　开展指挥信息系统安全防护实战化演练，提高应对网络攻击临机处置能力

在指挥信息系统常态化管理中，坚持全时段监控网络安全，定期进行风险评估，实时处理通报安全事件。每年举行带战术背景的防网络攻击实战演练，着重检验和提高三种能力：一是侦察预警能力。系统管理人员熟练掌握安全设备参数配置，确保策略恰当和安全系统正常运行，及时掌握系统告警信息，结合安全日志、审计信息等，对系统异常情况早发现、早处理，提高系统管理者对网络安全态势的感知能力。二是网络安全的控制能力。系统管理员在发现攻击行为后，通过网络工具迅速确定攻击源、攻击途径、危害性质及等级，采取果断措施，如切断网络、断开设备、推出系统等，把危害控制在最小范围，同时用杀毒软件等工具，清除有害程序。三是攻防对抗能力。依托训练基地与安全防护中心展开多回合的网络攻击和防御演练，围绕薄弱环节真攻真防，锻炼提升指挥信息系统保障部分队的应变处置能力。

4 结束语

随着指挥信息系统应用的深化拓展，指挥信息系统面临的网络威胁也在不断衍生发展，没有绝对的安全，只有不断提升系统网络安全防护能力。从指挥信息系统的软硬件基础设施、顶层体系结构设计、安全防护体系建设、系统使用和技术保护保障人员的综合素质提高等各个方面，综合施策，才能不断提高指挥系统的生存能力，确保系统稳定可靠运行。

参 考 文 献

[1] 任连生. 基于信息系统的体系作战能力概论[M]. 北京：军事科学出版社，2009.

[2] 徐小岩，许金裕，等. 计算机网络战[M]. 北京：解放军出版社，2002.

[3] 张应福. 云计算技术及其在下一代数据中心建设中的应用[J]. 通信与信息技术，2011，189（1）:39-42.

[4] 柴晓路，梁宇奇. Web Services 技术、架构和应用[M]. 北京：电子工业出版社，2003.

[5] 孟凡松，韩沂宁，周谷. 美军网络战体系建设策略及现状分析[J]. 航天电子对抗，2012（04）.

[6] 卢昱，张伶，等. 网络战装备概念和体系结构研究[J]. 计算机工程与科学，2006（02）.

[7] 伏晓，蔡圣闻，谢立. 网络安全管理技术研究[J]. 计算机科学，2009（02）.

[8] 穆军林，朱国阳，王江涛. 美军“舒特”系统攻击方式及应对措施[J]. 装备制造技术，2012（09）.

[9] 王巍. 解析美国成立网络战司令部[J]. 国防科技工业，2009（07）.

[10] 陆益敏，陈晓明. 美军C4KISR系统发展特点[J]. 国防科技，2006(12).

网络空间中指控需求的几点思考

牟其林，李　姝，李小花
（中国电子科技集团公司第三十研究所，四川成都　610041）

摘　要：伴随军队武器装备信息化程度的与日俱增，网络空间在军事领域的作用日益突出，网络空间战必将成为未来的主要战争形式之一。指控系统作为网络空间战的神经中枢，对取得网络空间战的胜利发挥着至关重要的作用。文中简述了网络空间概念、要素以网络空间带来的挑战，在此基础上，从安全防护、态势感知、资源调度三个方面分析了网络空间中的指控需求，以期对网络空间中指控系统的建设提供借鉴。

关键词：网络空间；指控系统；安全防护；态势感知；资源调度
中图分类号：TP3　　**文献标识码：**A

On the Demand for Command and Control in Cyberspace

MOU Qi-lin，LI Shu，LI Xiao-hua
（The 30th Research Institute of CETC, Chengdu Sichuan　610041, China）

Abstract: Cyberspace is becoming more and more important for the military, along with the growth of weapon and equipment informatization. Cyberspace would become one of the major warfare forms in the future. As the nerve center of the cyberwar, command and control system plays a vita role in the victory of cyberwar. This paper describes the concept and elements of cyberspace, and also describes the challenges faced by cyberspace. On the basis, it studies the demand for command and control in cyberspace, mainly including security protection, situational awareness and resource scheduling. This study is expected to be good for the development of our command and control system in cyberspace.

Key words: cyberspace; command and control system; security protection; situation awareness; resource scheduling

0　引言

网络空间已成为与陆地、海洋、空中、太空并列的一片新疆域，也是覆盖面最广的疆域。从计算机诞生之日起，以计算机和网络为基础的信息系统就逐渐发展起来，其上的软件和资源也不断丰富，最终形成了网络空间。

随着美军武器装备和作战理论的不断发展，“网络空间战”从设想开始走向现实。与传统的“平台中心战”相比，在“网络空间战”中指挥控制系统“战斗力倍增器”的作用将更加突出，对作战的影响也更加巨大[1]。

在未来的现代化战争中，网络空间中的指挥控制应有它自身的特点和关注点，文章将对此进行初步的分析和解读。

1　网络空间简述

从理论上讲，网络空间是所有可利用的电子信息、信息交换及信息用户的统称。网络空间已成为由计算机及网络构成的数字社会的代名词。

美国《第 45 号国家安全总统令暨第 23 号国土安全总统令》中将网络空间定义为：信息技术基础设施和相互依存的网络，包括互联网、电信网、电脑系统以及重要产业中的处理器和控制器，通常还包括信息虚拟环境以及人与人之间的互动。

1.1　网络空间的要素

网络空间具有四个要素：通信设备和线路；计算机；软件；数据通信与资源共享。

（1）通信设备和线路：是网络空间的基础设施之一，具体包括路由/交换设备、有线/无线通信设备、线缆等。

（2）计算机：是网络空间的基础设施之一，具有计算、存储和数据处理等能力。

（3）软件：是网络空间的核心支撑部分，通信设备和计算机中均运行着各种功能的软件系统。

作者简介：牟其林（1970—），男（汉族），重庆梁平人，高级工程师，大学本科，主要研究领域为网络管理、综合运维。E-mail：345900140@qq.com。

（4）数据通信与资源共享：是网络空间具备的基本能力，为各类各级用户提供所需的信息。

1.2 网络空间带来的挑战

现代信息技术的发展不可避免地会给军事通信系统带来新的理念及发展思路。

短短几年，网络空间已发展成为生存新空间和作战新领域，成为“信息控制”的全域空间。

在军事信息系统中，指挥控制系统是 C^4ISR 系统的核心，是作战指挥的神经中枢，是取得战争胜利的关键，所有的信息系统都是围绕它服务的。在网络空间中，指挥控制的区域前所未有的扩大，涉及海量信息的存储、处理和分析，涉及各种通信手段，涉及各类各级用户，面临更大的安全威胁……

2009 年 6 月 23 日，美国当任国防部长罗伯特·盖茨正式发布命令建立美国“网络空间司令部”；2010 年 5 月 21 日，该司令部正式启动，隶属于美国战略司令部。网络空间带来的军事变革由此拉开了序幕。

2 网络空间中的指控需求

在网络空间这一辽阔的新疆域中指挥作战，必然需要多个军兵种联动，首先应当具备安全防护能力，提供多级安全保障，其次必须掌握战场态势，另外还必须具有资源调度能力等，能够为一体化联合作战提供支撑。

2.1 网络空间中的安全防护

安全防护是指通过采用各种技术和管理措施，保护网络系统的硬件、软件及系统中的数据，使其不因偶然的或者恶意的原因而遭受到破坏、篡改、泄露，使得系统能够连续可靠正常地运行，网络服务不中断[2]。

网络空间指挥作战中，各类指控信息的产生、存储、传输和使用的全过程，均面临着这样或那样的安全威胁，传统的冲突形式已扩展到网络空间。

正确的指挥信息应当由合法的用户产生，应对各级指挥员进行身份认证。如果指挥所的指挥信息系统被敌军黑客攻击成功，就可以接替指挥权，获得作战指挥相关的重要信息，了解我军的作战意图和计划，并进行恶意篡改，进而发出对我方不利的指挥命令。

指控信息存储、传输的过程中，如果被敌军截获，也会对战局产生非常不利的影响。首先，应采取技术手段，尽量降低信息被截获的风险；其次，有必要对信息进行存储加密或传输加密，并对数据完整性进行保护，即便信息被敌军截获了，也要确保信息不会被破译或篡改。

安全防护技术和攻击技术一直在共同发展着，“矛”与“盾”的较量自古就有。虽然美军不断通过各种渠道表态，宣称美军网络空间行动的“核心是防御网络攻击行为，防御能力是其他一切作战能力的基础”[3]，但稍加分析即可看出，美军在网络空间要达成的目标是：攻防结合，构建网络威慑体系，在军事上巩固自己的“制网权”。美国国防部副部长林恩曾明确表示，美方将保留回应严重网络攻击的权利，会在“我们选择的时间和地点做出相称且正当的军事回应”[4]。前任国防部长帕内塔曾指出：“现在我们生活在一个完全不同的世界里，要面对可与珍珠港比拟的网络空间攻击”，“我们必须做好应对准备，在网络空间，我们要同时拥有良好的网络进攻与网络防御能力”[5]。这些讲话充分显示了美军注重网络空间威慑效应、在网络空间强调攻防结合、必要时不惜主动发动网络攻击的心态，其军事目标绝不仅仅是保证自身网络安全，而是要通过提升网络攻击能力劝阻和威慑所有不利于己的网络攻击行为，实现其在网络空间的绝对自由、绝对优势和绝对安全[6]。

在网络空间中，国家与国家之间的攻防演练也从来没有停止过。2008 年 7 月，俄罗斯利用攻击软件的隐蔽注入，对格鲁吉亚实施了全面的网络攻击，导致网络瘫痪。2011 年 12 月，伊朗宣称其“电子战部队”用“黑客劫持”的方法使得美国的一架 RQ-170 隐形无人机脱离航线，降落在伊朗境内。2012 年 5 月被发现的“超级火焰”病毒在中东大范围传播，在计算机内隐蔽驻留、窃取数据。2014 年 3 月，俄罗斯总统官网遭遇网络攻击。从历次的网络攻击事件来看，网络攻击效果不亚于常规武器的火力打击。网络空间的安全，就是国家的安全，网络空间已成为国家主权领域空间。

2013 年 11 月 12 日，十八届三中全会成立了“国家安全委员会”，该委员会是继党中央、国务院、全国人大、全国政协之后，我国的第五大国家机构。2014 年 4 月 15 日，习近平主席主持召开了中央国家安全委员会首次会议，这标志着国安委开始正式运转，安全已成为国家战略层面重点关注的问题。

如图 1 所示，网络空间中的安全防护应采用多级安全保障机制。在国家战略层面，是国家级网络安全防护；在关键部位，有军队、政府、经济等领域的网络安全防护；在大型企业中，有国有、私有等企事业单位的网络安全防护；在局部，有个人、家庭等范围的网络安全防护。其中，国家层面的安全防护主要包括边界网络安全和骨干网络安全；企业级（及军队）安全防护主要包括边界网络安全和内网安全；个人计算机安全防护主要包括计算机终端安全、终端软件安全及终端数据安全。在不同的安全级别上，保护的信息内容各不相同，大到国家战略规划、发展路线，小到个人隐私、银行密码等。信息的泄漏，无疑会对国家、企业、个人的生存和发展带来打击和负面影响，甚至会破坏国家的安全和稳定。