中国科协学会学术部 编

新观点新学说学术沙龙文集 100

国土信息安全与异地容灾备份

中国科学技术出版社
CHINA SCIENCE AND TECHNOLOGY PRESS

新观点新学说学术沙龙文集 ⑩

国土信息安全与异地容灾备份

中国科协学会学术部　编

中国科学技术出版社
·北　京·

图书在版编目（CIP）数据

国土信息安全与异地容灾备份 / 中国科协学会学术部编 .—北京：中国科学技术出版社，2015.12

ISBN 978-7-5046-7017-5

Ⅰ .①国… Ⅱ .①中… Ⅲ .①国家安全—信息安全—研究—中国 Ⅳ .① D631

中国版本图书馆 CIP 数据核字（2015）第 269299 号

选题策划 赵 晖
责任编辑 赵 晖 夏凤金
责任校对 何士如
责任印制 张建农

出 版 中国科学技术出版社
发 行 科学普及出版社发行部
地 址 北京市海淀区中关村南大街 16 号
邮 编 100081
发行电话 010-62103130
传 真 010-62179148
投稿电话 010-62103182
网 址 http：//www.cspbooks.com.cn

开 本 787mm × 1092mm 1/16
字 数 150 千字
印 张 10
版 次 2015 年 12 月第 1 版
印 次 2015 年 12 月第 1 次印刷
印 刷 北京长宁印刷有限公司

书 号 ISBN 978-7-5046-7017-5 / D · 98
定 价 18.00 元

序 言

《国土信息安全与异地容灾备份》一书，经过大家的共同努力终于和读者见面了。本书是2015年7月18-19日由中国科学技术协会主办、中国国土经济学会承办的第100期新观点新学说学术沙龙“国土信息安全与异地容灾备份”的研讨成果汇编，可以说基本上反映了该领域的最新学术和思想动态。

“国土信息安全与异地容灾备份”包含着多个关键词。首先是“国土”。关于国土，有多种认识，可以仅仅理解为国家主权所管辖的陆地和海洋空间，也可以理解为包括土地、水、矿产、生物和气候等资源在内的一个国家可以自主管控的自然资源综合体。其次是“信息”。我们正处在并将长期处在一个信息多源生成、快速传输、竞相收集的信息时代，信息安全关系国家和地区安全，关系企业和事业单位发展，关系个人和家庭安全隐私。第三是“安全”。安全是系统的、多维的。根据2015年7月1日开始施行的《中华人民共和国国家安全法》，国家安全主要包括政治安全、国土安全、军事安全、文化安全、科技安全等11个领域。第四是“容灾”。容灾其实就是容忍灾难，或者说在灾难袭来时，能做到从容不迫、应对自如，不造成或较小造成损失。这里的灾，既指“天灾”即地震、洪涝、火灾等自然灾害，也指信息失灵、系统缺陷、设施缺失、操作不当、恶意攻击等造成的“人祸”。最后是“备份”。备份就是事先准备好另一套完整的方案、设备、人力等，时刻准备着用B计划或B方案、B系统迅速、安全、无缝地替代A计划、A方案、A系统。

从上面对五个关键词的解析不难发现，“国土信息安全与异地容灾备份”关系国家安全，特别直接关系国土安全、信息安全、资源安全，也间接地关系到国家军事安全、经济安全、社会安全和生态安全。我国国土辽阔、边境线长、资源丰富、生态多样，资源安全、生态安全和国土安全等面临诸多挑战，包括资源、环境、生态、边境等在内的国土信息，长期以来为国际力量所关注。保障国土信

息安全，既是国家资源安全的需要，也是保障国土安全、生态安全的需要。我国政府高度重视国土信息及其安全问题，包括国土资源部、水利部、国家海洋局、国家林业局、环境保护部等部门都设有专门的信息机构，对于国土信息化管理起到了重要的支撑作用。然而，不可否认，我国国土信息领域还存在诸多问题，信息的及时性、准确性、公开性问题较为突出；同时，关系到国土安全及资源安全的关键国土信息的安全问题也须进一步予以重视。国土信息系统容灾能力建设问题更是迫在眉睫。保障国土信息安全，迫切需要建立国土信息（异地）容灾备份（系统）。显然，研究这样一个课题具有十分重要的意义。

据我所知，国内对于信息系统容灾能力建设越来越重视，包括金融、电力等关键行业的信息系统容灾备份开展得比较早，技术方案等也较为成熟有效。然而，国土信息系统的容灾备份起步较晚、进展较慢、水平较低。对国土信息安全性的认识不足是其主要原因。同时，国土信息（系统）安全往往以隐性漏洞（隐患）为主，造成敏感国土信息的流失，对于国土安全等造成不同程度的损害。加强国土信息安全能力建设，特别是加强国土信息安全备份系统建设，是我国国土安全、信息安全的必然要求。

应邀参会的各位专家学者围绕“国土信息安全与异地容灾备份”这一主题，阐述了各自的理解和认识、研究和成果。其中，关于第四国土空间的论述，增加了对国土空间的信息空间认识维度，相信对于增进国土信息及其安全的认识是有益处的；关于国土信息安全备份系统建设需要从硬件、软件和人力等多个方面入手的认识，以及技术、设备和管理并重的认识，也是契合我国目前国土信息安全现状和保障我国国土信息安全需要的；关于适应信息科技发展趋势，特别是要适应云计算技术的发展趋势，努力建设和应用“国土资源云”的认识及倡议，具有较强的针对性和可操作性，相信也会引起我国国土部门的重视；关于妥善地处理好国土信息安全与公开关系的共识，有助于我们科学、审慎地甄别、处理国土信息安全与公开的关系，该公开的一定要公开，该保密的一定要保密，决不能以公开否定保密或以保密否定公开；有学者对海洋国土信息安全问题做了专门的讨论，相信对于保障我国海洋国土安全、发展海洋经济、建设海洋强国也是有裨益的；有学者专门对信息灾备等级和灾备市场进行了系统分析，提出不能无限地进行灾备，而要经济合理地开展包括国土信息灾备在内的灾备体系的建设；有学者

对构建我国国土信息安全保障体系做了分析和展望；有学者特别提及我国有的地方政府成立了“数据统筹局”，以加强对政府数据的统筹管理和服务；还有学者谈到了“数据伦理”的问题，认为数据的生成、传输、使用等都要讲道德、讲规矩。凡此种种，学者的观点很新颖、很有启发，相信对我国国土信息事业的持续健康发展是很有益处的。

当然，“国土信息安全与异地容灾备份”目前还是一个新领域、新课题，在我国尤其如此，还有许多问题没有搞清楚、研究透，特别是在此次讨论会上我们经常会听到“我不是 ×× 方面的专家”，这恰恰说明了国土信息安全及其容灾备份是一个跨学科、跨领域的课题，需要包括国土、信息、管理、技术等多领域、多学科专家学者、企业和管理工作者的共同努力。

最后，需要特别说明的是，本书所汇编的专家学者的观点也不一定都是正确的、准确的。我们不去对这些观点的“正误性”过分追究，只是想以此书唤起专家学者的注意和兴趣，让我们共同致力此领域的研究与实践，共同为国家安全、国家建设服务。

谷树忠

2015 年 8 月于北京

谷树忠，中国国土经济学会常务理事，国务院发展研究中心资源与环境政策研究所副所长、研究员、博士生导师。

目　录

主题一：国土信息安全与第四国土空间

时　间：2015年7月18日上午

地　点：北京

主持人：陈荣国

柳忠勤（中国国土经济学会副理事长兼秘书长、研究员）：

党的十八大报告明确提出要把信息化纳入全面建成小康社会的目标，信息化建设定将成为推动我国各项事业长期发展的必要手段。2015年7月1日正式发布并生效执行的《国家安全法》中专门提出国家要建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及技术的安全可控，维护国家网络空间主权、安全和发展利益。

随着国土信息化建设的深入，对数据的持续保护刻不容缓，异地容灾备份对国土部门，保障数据信息安全和提高关键数据的使用效率极为重要。在这种大背景和需求下，我们举办本次沙龙意义和影响力十分深远。

由于本次沙龙主题的理论性和实践型都很强，所以我们除了邀请领域内科研机构及专家学者参会外，还特别邀请了在软件关键技术、信息数据系统建设及数据库建设与管理方面业绩和经验丰富的国建正坤数字科技（北京）有限公司、迪思杰（北京）数据技术管理有限公司等企业参与协办。他们和在座的很多企业一线信息安全专家都是从事容灾备份落地具体工作的，实践经验十分丰富。

我们认为，就沙龙要解决的问题而言，产学研一体的研究探索才是方向，才有意义。相信大家在会议交流活动，争辩质疑的讨论中定能碰撞出思想火花、关键学说、解决方案等成果，为中国科协、国家相关部委和领域建言献策。

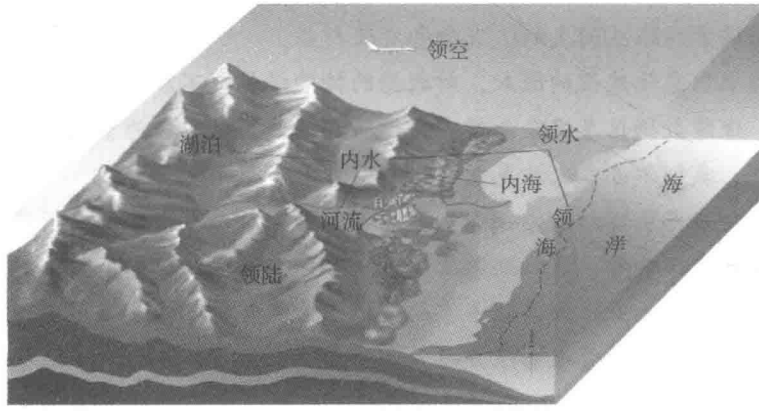
第四国土空间安全

◎ 陈荣国

我从五个方面谈谈第四国土空间安全问题。

一、第四国土空间解析

第四国土空间是非常新的概念。国土就是国家领土，国家领土分为领陆、领水（包括内水和领海）和领空三个部分，上及高空，下及底土。领水附随于领陆。领空和底土又附随于领陆和领水。领陆变动时，领水、领空和底土亦随同变动。国家势力范围在物理上还可扩张到太空、深海和极地。



随着信息技术的迅猛发展和应用，网络空间的地位日显突出。新的国家安全法明确了网络空间主权的概念，网络空间的安全已成为新时期国家安全的焦点。这个新兴的具有国家主权的空间称为第四国土空间——领网，与领陆、领水、领空并列。

这个新空间可延伸为网络电磁空间。它是融合物理域、信息域、认知域和社会域，以互联互通的信息技术基础设施网络为平台，通过无线电、有线电信道传递信号、信息，控制实体行为的信息活动空间。电磁空间涉及面太广，本沙龙将聚焦讨论网络空间。

二、有关信息安全的几个概念

（1）信息安全可以理解为保障国家、机构、个人的信息空间、信息载体和信息资源不受来自内外各种形式的危险、威胁、侵害和误导的外在状态和方式及内在主体感受。可指线下和线上的信息安全。

（2）网络安全侧重点是线上安全和网络社会安全。

（3）网络空间安全侧重点是与陆、海、空、太空等并行的空间概念。

（4）信息主权是信息时代国家主权的重要组成部分，是国家对本国的信息传播系统和传播数据内容进行自主管理的权利。包括：对本国信息资源进行保护、开发和利用的权利；自主确立本国信息生产、加工、储存、流通和传播体制的权利；对本国信息的输出和外国信息的输入进行管理和监控的权利。

（5）信息边疆是国家或政治集团信息传播力和影响力所能达到的无形空间，是在电磁和网络空间被各个不同的网络拥有者所防卫的主体疆界。

三、“领网”安全的四域

1. 物理域

物理域的基础是网络基础设施及其拓扑结构。物理域的安全指的是网络硬件设施与设备的安全，确保其不被干扰、破坏和摧毁。

2. 信息域

信息域主要收集、处理、存储、分发、显示和保护信息，是物理域与认知域的连接桥梁。信息域的安全主要指网络信息安全，包括：①完整性：保持信息原样性，不被修改、破坏和丢失；②保密性：杜绝有用信息泄漏给非授权个人或实体；③可用性：信息传输与运行正常，并具备可恢复性；④不可否认性：保证所提供信息的真实同一性；⑤可控性：任何信息要在一定传输范围和存放空间内可控。

3. 认知域

认知域主要体现参与人员的认知，包括感知、意识、理解、决策、信念和价值观。认知域安全主要包括政治安全、道德安全和心理安全等。主要是有关传播信息内容对国家政治以及对人们的思想、道德和心理等方面的影响。

4. 社会域

社会域体现的是个体认知扩散和群体性共同认知。社会域安全是关于网络空间安全对社会安全的影响，要求确保不因网络问题而出现经济安全事件、民族宗教事件、恐怖事件以及群体性事件等社会事件。

四、网络空间安全现状

国际上对网络空间安全最重视的是美国。美国于2003年出台了《确保网络空间的国家安全的战略》，2006年制定了《网络电磁空间作战国家军事战略》，2009年出版了《国家网络安全战略报告》，同年成立了网络电磁空间司令部，2011年宣布了《网络电磁空间国际战略》，并发展了网络数字大炮、僵尸战略等网络武器。

欧盟对网络空间的安全也非常重视，2004年成立了欧洲网络与信息安全局，推动了可信计算、电子追踪等项目研究。俄罗斯、日本、印度、巴西等国也相继进行了网络安全立法，并建立了相关管理机构。

我国在新时期对网络安全也比较重视，党的十八大明确提出了网络空间安全、信息安全和太空安全等概念。在2014年中央网络与安全信息化领导小组第一次会议上，习近平主席指出，“没有网络安全就没有国家安全，没有信息化就没有现代化”。2015年新的《国家安全法》颁布，维护国家网络空间安全主权成为亮点。另外，《网络安全法》草案已经开始在人大征求意见。

但在技术层面，我国网络空间的核心技术依然掌握在欧美发达国家手中，网络空间缺乏顶层设计，网络安全产品过于依赖进口，难逃类似棱镜门之类的威胁。我国“领网”安全面临着巨大的挑战。

五、“领网”安全战略考虑

在信息安全战略层面，必须加快制定和颁布国家层面的网络与信息安全战

略，力争参与制定国际网络空间的规则。在技术层面，应尽快提升我国信息安全的自主可控水平，建立安全可操纵的网络安全信息保障体系，提高网络空间安全的保障能力。从处理芯片、操作系统、数据库管理系统、中间件和应用软件等层次，构建自主可控的高安全应用体系，建设具备感知能力的网络防御与对抗体系。

乔惠民：

刚才陈老师讲得非常好，第四国土空间这个概念，是从主权的角度提出的，领土的空间、领海的空间、领空的空间，这是一贯的概念。现在所提的第四国土空间也就是国土第四空间，提法和语义是一致的，这是一个虚拟的空间，即国土信息化空间，我们以往虽然从大国土的角度涉及了这个概念和提法，但是都还不够完整和系统，今天陈老师比较完整、深入地阐释了这个新的概念，我很支持。

最近在《国家安全法》里也提出了一个很重要的概念，恰好是围绕网络提出的，叫作网络空间主权。因为国土空间问题，对一个国家来说首先是要强调主权，比如空域的主权、海域的主权、陆域的主权，顺应信息化时代发展，现在也提出了网络空间主权概念，所以国土第四空间——即信息化空间安全的概念，跟我们《国家安全法》强调网络空间主权的法律要求是一致的。

我们今天主要讨论信息安全、容灾备份的问题，而一上来却讨论国土的第四空间的概念，我觉得从这个角度切入是非常有意义的。因为《国家安全法》是2015年7月1日颁布的，《网络安全法》草稿现在是人大征求意见稿，这两个法也应该是我们这次开会的指导方针。因为现在加强网络空间、信息空间安全，是一件非常重要的事情。

陈荣国：

乔老师说得很有道理，只要在互联网上的信息，其安全都面临威胁。目前美国国安局可以破译几乎任何长度的密码。几十位甚至上百位的密码都可以暴力破解。

换个角度看，网络空间也是一个实在的空间

◎ 于大鹏

我有几个观点跟大家分享一下。

第一，“领网”是一个很好的概念。大家通常会说网络是虚拟空间，但我认为可以把它看成实体空间。因为这个空间里有容量，也在消耗能量；可以救人，也可以杀人，也就是说在这个空间里可以达成生意，也会破坏社会治安。所以，从这个角度看，网络空间已经不虚了，已经非常实在了。在这个实在的空间里，它的破坏力可能更大、建设力可能更大，如瞬间就可以将信息传送到世界各地。所以我希望大家可以改变一个观念，就像电磁波一样，虽然我们看不到，但是它是实实在在存在的一个场。网络空间也是实实在在存在的。这样，我们看待问题的思路可能不一样。

第二，如果这个空间和以往建的空间不一样，我们思考的方式就不一样了。社会发展大概经历了农耕社会、工业化社会和现在的信息社会三个阶段。因为我国在农耕社会待的时间太长，所以我们的很多思维会站在农耕社会的角度。农耕社会叫自给自足，盖一个四合院，我们就认为别人进不来，就像古代建的长城一样。到了工业化社会已经是全球社会化分工，到了网络社会更是地球村。站在这个角度分析问题，我们再用农耕社会的思维来管理我们信息化社会的事，就不合时宜了。比较典型的是我们各行各业，包括军队都是做物理隔离，用物理隔离来保证信息安全。这完全是农耕社会思维，这个实实在在的网络空间已经不是我们能够用长城来阻挡的。以为如果做了隔离，别人进不来，但是任何一个节点都可以把信息泄漏出去，而且是在我们不知不觉的情况下。打一个比方，就像一个孩子出生的时候，我们放在一个无菌室里，没有见过世面、没有经过风雨，任何一点儿细菌就能让他死亡。所以，我觉得做物理隔离是非常危险的事，完全是用农耕社会的思维来经营网络空间，这件事情我在几个场合也谈过这个问题，但是好

像大家没有认识到，认为这是最安全的。我觉得到目前为止是一个非常大的一个漏洞，而且是一个非常危险的思维方式。我跟大家分享一下，大家思考是不是存在这个问题。

我的想法是，像我们这样的单位最好能够开放，因为我们现在上网上不了，也就是说这些搞网络攻防的学生们没有实战经验去跟别人对抗，以后会是一个什么情况？我们就没有战场。实际上现在战场处处存在，但是我们这些人就关在屋子里根本打不了仗，所以我认为这是一个非常大的缺憾。

陈荣国：

物理隔离是没办法的办法。

陈红梅：

我是航空测评分中心的，是中国第一家从事行业涉密网络管理的机构。实际就是国家保密局，代表国家，10 年前走到一个比较明确的地位，来行使国家保密管理的部门。我要说的一是，物理隔离是国家的管理决策。于老师说物理隔离免疫能力不够，我们也有体会。2006 年开始按照分级保护标准来建设涉密网络，10 年后按等级保护标准建设互联网的时候，发现我们的抗攻击能力的确是差的。所以涉密网络物理隔离是一种无奈的选择，也是目前国家保密法所明确要求的。

二是，网络真的物理隔离了吗？刚才乔老师提到，其实情报窃取泄密渠道是很多的，我们的技术很局限，核心技术又受制于人，斯诺登事件就暴露了很多突破物理隔离的方法。WIN10 就是用一种你很舒服很没有防卫的，很自然的、觉得就是在享受服务的同时，把你的个人计算机工作环境迁移到云网络了。

三是，规范化管理需要更精准的标准。我想再次表达我们一线人的诉求，就是需要更多操作层的解决方案，因为企业没有这么多的专家，没有这么好的研究能力，更多是你告诉我做什么，我按照规定来做。国际性的标准在我们这儿怎么落地？10 年前的标准与现实应用产生了适用性的问题，所以国家保密局已经启动了一个项目来进行部分标准的修订，但在修订过程我们发现需要更多领域的专家的参与才能保证新出台标准的完备性和实用性，真的需要科技圈里的专家们多多参与多多指导。

四是，我认为人员的安全保密意识教育是治根之举。我们10年前开始更加密切关注泄密的管理，但是现在泄密事故却频发，尽管现在涉密管理更严格了，可是对有些人，很有限的金钱就能够被买通。运动式的保密工作已经比较“热闹”了，怎么做一些有实效的工作需要思考并关注。

张祖国：

我是来自中船重工集团公司船舶信息中心的张祖国。目前，一方面协助做集团内成员单位的信息安全系统规划与建设工作，另外也参与IT产品的研发。我的感受就是跨界的信息安全人才需求非常大。

这两年在推动去IOE过程中，国内安全厂商是最大的受益者。但是在国内信息安全体系建设中，我认为最大的失位者，没有承担起责任的，也是国内的部分信息安全厂商和集成商。刚才于老师也提到，咱们用长城的方式防守是过去的农耕时代，如果一个单位的信息安全人才非常丰富，水准非常高，而且他能够充分理解企业的需求，并且如果把它抽象成一个很好的策略，那么整个安全体系构建就会相对完善。如果人才缺得比较厉害，赶上集成商水平又比较弱，情况就会很值得担忧。

现在很多厂商更多是把他们的设备调调就行了，似乎认为设备调试就是最基本的任务，但是针对安全策略整个体系的构建，绝大多数信息安全厂商所谓的资深安全工程师水平都不够理想，应该说提升的空间非常非常大。所以说，当厂商的工程师如果只停留在设备这个级别，而不融入行业安全需求，实际上对行业信息安全的责任没承担到位。

这是我说的第一个观点，最大的受益者和最大的失位者——国内的信息厂商需要做的工作还非常多，绝对不能利用开源代码改改就卖给用户，原创的成果还远远不够。

第二，刚才提到信息安全不是简单地只是买一大堆先进的设备，更要从人才角度、从信息技术和业务系统的融合跨界的分析，以及后续信息安全日常运维体系，构造一个完整的体系。

第三，刚才陈老师提到的我非常同意。信息安全标准，往往只能提供相对宏观的视角和比较概要的目标，技术解决方案不断在改变。研究发现，无论是开源

的微服务架构，还是软件定义网络、虚拟化部分，实际上根据我们的信息安全标准，能找到可行的解决方案还是比较少的。标准需要不断根据技术进行调整，而技术研发要走的路还是比较长。

赵建安：

我是中科院地理资源所的，跟陈教授是一个单位。针对陈教授的发言，我想到两个问题：

第一，所谓“空间领域”的问题，我们要提出一个新的概念的时候，在学科角度可能需要在哲学上找它的立足点，如果能够总结出立足点，这个概念就能比较好地总结出来了。这一点涉及第四空间是否成立的问题，这个确实很重要，因为后面涉及一系列的问题，包括前面陈红梅女士提到的网络信息空间立法的问题，为什么立法工作做不起来？实际上没有把基本概念和内涵搞清楚，所以后面跟着一系列要出问题。不仅仅是一个网络的问题，实际是整个信息安全的一个基本体系、基本研究的工作，可能我们没做上去，更不要说国土信息安全的工作。

第二，我不是信息安全方面的专业人员，只能从宏观层面提点自己的看法。刚才于教授提的信息工程的问题，我非常同意。网络信息安全出问题出在什么地方？我觉得可能有两个方面：一个是节点上的，一个是里面的参与者的问题。如果人不可靠，光靠硬件怎么安全？这肯定是一个非常重要的问题；另外一个可能出现问题的，我们讲安不安全，应该在传输过程中，我理解的是国防军事上应强调“制电磁权”，把“制电磁权和制信息权”等同起来。如果是“制电磁权”的话，实际上它的传播不是一个可以物理隔离的有线传播，它涉及空间传播，空间传播就意味着只要你控制这个频段信号就能够找到它的切入点，这一点可能是出在传输过程中。网络空间最主要的是无线空间，如果这一点做不好肯定就会出问题。

另外谈一点看法，我以为信息安全不完全是一个保密的问题，可能更多首先是从信息的搜集开始，包括信息的制作、集成、传输的整个过程，这里面还包括信息的真实性问题，就涉及它是否安全的问题。我举一个最简单的例子，我们国家的土地资源状况，比如说某城市开发土地状况，对现有土地的实际变化状况，连管理部门自己都扯不清楚，还是在保密的情况下，就出现数据在两个相邻年际之间的变化幅度之大，你的数据都不真实，还谈得上安不安全吗？！