# 浅谈电子政务建设中的信息安全问题

文／张生霞·湖南省娄底市委党校

在经济和信息全球化加速发展的前景下，电子政务逐渐成为各国政府发展经济、增强国际竞争力的“好帮手”。然而政务信息的公开化、社会化，同时也给不法之徒开启了“入侵之门”。电子政务的信息安全问题备受人们关注。理解电子政务信息安全的概念，认识电子政务信息安全的威胁，把握电子政务信息安全的要求，树立正确的信息安全观，才能真正做到“一网管天下”。

电子政务是指政府机构运用现代信息与通讯技术，将管理与服务通过信息化集成,在网络上实现政府组织结构和工作流程的优化重组，超越时间、空间和部门分隔的制约，全方位地向社会提供高效优质、规范透明的管理与服务。电子政务的建立将使政府成为一个更符合环保精神的政府，一个更开放透明的政府，一个更有效率的政府，一个更廉洁勤政的政府。然而，电子政务的职能与优势得以实现的一个根本前提是信息安全得到有效保障。因为电子政务信息网络上有相当多的政府公文在流转，其中不乏重要信息，内部网络上有着大量高度机密的数据和信息，这些信息直接涉及政府的核心政务，它关系到政府部门、各大系统乃至整个国家的利益，有的甚至涉及国家安全。如果电子政务信息安全得不到保障，电子政务的便利与效率便无从保证，对国家利益将带来严重威胁。因此说，电子政务信息安全是电子政务建设与发展过程中必须解决的首要问题和核心问题。

## 一、电子政务信息安全的概念

电子政务的信息安全可以理解为：

(1)从信息的层次看，电子政务信息安全包括信息的完整性(保证信息的来源、去向、内容真实无误)、保密性(保证信息不会被非法泄露扩散)、不可否认性(保证信息的发送和接收者无法否认自己所做过的操作行为)等。

(2)从网络层次看，电子政务信息安全包括可靠性(保证网络和信息系统随时可用，运行过程中不出现故障，遇意外事故能够尽量减少损失并尽早恢复正常)、可控性(保证营运者对网络和信息系统有足够的控制和管理能力)、互操作性(保证协议和系统能够互相联接)、可计算性(保证准确跟踪实体运行达到审计和识别的目的)等。

(3)从设备层次看，电子政务信息安全包括质量保证、设备备份、物理安全等。

(4)从管理层次看，电子政务信息包括人员可靠、规章制度完整等。

信息系统安全的强弱遵循“木桶效应”，任何一个环节上的疏忽，都将有可能导致不可挽回的损失，因此电子政务信息安全问题必须系统地加以解决。

## 二、电子政务信息安全的威胁

电子政务信息安全是一个复杂的系统工程。仅从安全威胁的来源来看，它可以分为内、外两部分。所谓“内”，是指政府机关内部；而“外”，则是指社会环境。来自于外部的威胁有病毒感染、黑客攻击、信息间谍、信息恐怖活动、信息战争、自然灾害等；而来自内部的威胁则包括内部人员恶意破坏、管理人员滥用职权、执行人员操作不当、内部管理疏漏、软硬件缺陷等。

一般说来电子政务信息安全中普遍存在着以下几种安全隐患：

**(1) 窃取信息**

由于未采用加密措施，调制解调器之间的信息以明文形式传送，入侵者使用相同的调制解调器就可以截获传送的信息。同时，政府机关内部人员更是可以十分轻松的将一些机要信息泄漏出去，此谓“监守自盗”。

**(2) 篡改信息**

当入侵者掌握了信息的格式和规律之后，通过各种方式，在原网络的调制解调器之间增加两个相同类型的调制解调器，将通过的数据在中间修改，然后发向另一端。这便严重地破坏了原信息的完整性与有效性。

**(3) 冒名顶替**

由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨。同时，由于内部权限分

配不明或者滥用他人名义实施违法活动，极有可能造成“栽赃嫁祸”。

**(4) 恶意破坏**

由于攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机要信息，甚至可以潜入两边的网络内部，其后果是非常严重的。如果政府内部人员发泄私愤或被外部不法分子利用，破坏重要信息的数据库或其他软硬件，那么这样造成的后果更是不堪设想。

**(5) 失误操作**

如果缺乏明确的操作规程和必要的备份措施，一旦出现失误操作，那么重要的信息将无法恢复。

## 三、电子政务建设的信息安全要求

**1. 系统运行的安全**

电子政务系统必须能够正常运行，能够支撑政务的正常履行。

**2. 系统内信息的安全**

系统内的信息要保密，要完整，要可控。

● 保密是指要有措施来防止别人窃取政府的秘密，要防止秘密从内部泄露出去。保密是政务信息的最主要的特点。

● 完整是指政务信息的完整性。政务信息涉及到政令，涉及到国民经济的运行，涉及到执法，涉及到政府对整个国家的管理，因而，对所有的信息一定要有防止篡改的措施，以防被人随意地篡改、删除。

● 可控是指这是政务信息的可管理性。电子政务简单地说就是把政府移植到网络上面，因此政府管理也相应地要移植到网络上。政府的管理是等级制，行政有级别，文件有级别，信息有知密的范围，政令有发放的范围和时间的要求，所以，可控就是要有确切的手段防止公务员在网络上打破政务管理层次，越权行事。此外，可控还指能够做到对不履行职责的，错误履行职责的，有据可查，以达到赏罚分明，职责分明。

**3. 系统管理控制的安全**

电子政务系统一定要完全归政府部门所管理、所控制，而不能被建设系统的公司所控制，更不能由外国的厂商、外国的机构所控制。

## 四、“一个基础、两根支柱”确保电子政务的信息安全

根据国家信息化领导小组提出的“坚持积极防御、综合防范”的方针，笔者认为应从三方面着手解决我国电子政务的安全问题，即“一个基础(保障)，两根支柱(技术，管理)”。

**1.支柱1——安全技术方面**

技术性的要求，涉及到政府、电子政务、网络运行安全的主要技术因素。笔者建议从以下几个方面来考虑：

**(1) 物理安全**

首先要加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞；其次要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出隐患，及时修补。

**(2) 访问控制**

建立完善的访问控制措施，如安装防火墙，加强授权管理和认证等。

**(3) 安装防病毒软件**

加强内部网的整体防病毒措施。

**(4) 通信保密**

对敏感的设备和数据要建立必要的物理或逻辑隔离措施。

**(5) 备份**

利用数据存储技术加强数据备份和恢复措施。

**(6) 安全管理**

建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

**2.支柱2——安全管理方面**

在电子政务的安全建设中，管理的作用至关重要。安全管理主要包括以下三方面：

**(1) 管理对象**

重点在与人和策略的管理，人是一切策略的最终执行者。

**(2) 管理内容**

● 核心业务层与外网隔离

党政军内部网络是我国信息网络的重要组成部分，按照2002年发过的17号文件精神，国务院办公厅把信息网络分为内网(涉密网)、外网(非涉密网)和因特网三类，

而且明确内网和外网要物理隔离。

● 政务系统中权限的控制

电子政务需要划分成若干个安全域，不同的安全域中，安全的要求、级别是不一样的，因此需要把使用不同级别政务信息资源的用户划分成不同类型，实现不同类型人员对不同级别信息访问的控制策略。

● 系统的安全备份与恢复机制

鉴于政务信息的重要性和特殊性，建立必要的备份制度和有效的系统和数据恢复机制是保障电子政务安全的基本需求。

● 定期检测和审计机制

对于电子政务系统运行中的漏洞以及工作人员在执行安全策略方面的疏忽必须通过制度来监控并且及时予以纠正。

● 信息发布严格合理审查机制

政府信息化的要求之一就是利用互联网络做强有力的宣传，同时从安全的角度，还需要防止敌对力量通过网络系统散布不满情绪、制造流言、做颠覆性的宣传等不利于政治与社会稳定的行为。因此，需要对发布的信息进行必要的审查，尤其是要看管好BBS系统。

● 废旧信息存储介质的处理

有关专家特别要强调利用废旧磁媒体获取信息的问题。一些技术可以从消过磁的介质（如磁盘、磁带和光盘等）中恢复曾经存储过的信息，因此某些情报机关就利用收集废旧物品的机会专门搜集废旧磁媒体，从中获取情报。所以，对废旧磁媒体要特别加强管理。

● 对管理机构的要求

建设电子政务一定要有明确的电子政务信息安全方面的管理机构。这样才能责任到人，职责到位，才能落到实处。

● 安全制度方面的要求

在安全管理中必须要有相应的安全制度。涉密的信息，上不上网，上什么样的网，进不进软盘，软盘怎么管理等等，以及前面讲到的信息安全的一些风险和隐患都要考虑进去。这些制度该学习的要学习，该贯彻的要贯彻，这样才能够把信息安全融进日常管理，使之真正起到作用。

**（3）管理步骤**

安全管理主要有以下三个步骤：

● 事前明确要求；

● 事中严格监督；

● 事后严肃惩处。

**3.基础——安全保障方面**

保障性的要求是保障网络日常的安全运行。

**（1）设备来源的安全性保障要求**

安全设备必须通过安全主管部门或是技术测评机构等国家有关部门认证，它的安全性才有保障。设备来源的安全要求是系统能不能安全的根源，就像建一栋大厦一样，每一块砖必须是合格的，钢筋混凝土必须是合格的。

**（2）系统运行的安全性保障要求**

安全运行需要定期对系统运行的状况进行评估和总结，检查运行是否正常，有哪些违规的行为，有哪些突发攻击事件，查看防火墙记录、入侵检测设备记录、审计记录，它们都告了几次警，自动生成了几次报告等等。

**（3）系统安全的应急性保障要求**

系统必须要有应急服务，一旦出现紧急情况如突然间停电了或者系统的一台机器坏了怎么办？一定要有预案，并且这个预案要经过实际的演练，在发生紧急情况的时候能起作用。

**（4）安全法律方面的安全性保障要求**

这方面的安全性保障要求主要有国家的相关管制法规、国家的相关行政法和有关部委的相关规章制度。

**现行部分计算机网络管制法有：**

●《中华人民共和国保守国家秘密法》第三章；

●《计算机病毒控制规定》；

●《计算机软件保护条例》；

●《中华人民共和国计算机信息系统安全保护条例》；

●《中华人民共和国计算机网络国际联网管理暂行规定》；

●《中华人民共和国计算机信息网络国际联网管理暂行规定实施细则》。

**现行相关行政法主要有：**

●《中华人民共和国行政许可法》；

●《中华人民共和国行政诉讼法》；

●《中华人民共和国行政复议法》；

●《中华人民共和国行政处罚法》;

●《中华人民共和国行政监察法》。

**有关部委制定的规章制度有**:

《国土资源管理系统行政为民措施》和《国土资源管理系统工作人员禁令》。这些规章制度都是比较有效保障网上政务安全运行的成功典范。

需要强调指出的是:信息安全需要三分技术、七分管理。因此,技术安全手段应当服从于和服务于管理安全手段。具体而言,技术手段只有和规章制度的有效执行相配合,才能产生信息安全效益。

## 五、树立辩证的安全观,实施务实的策略

理解电子政务的信息安全问题,应从社会发展这个层面来理解。

第一,要处理好发展和安全的辩证关系。安全是为发展服务的。此外,信息安全是发展的概念,今天的安全不等于明天还安全,不存在绝对的安全。

第二,网络与信息安全不是局部的安全,它是一个综合的安全,牵扯到人,牵扯到技术,牵扯到网络的运行。

第三,网络安全是相对的安全,永远没有绝对的安全。信息安全的对策应是风险的管理和控制。因为技术在不断发展,影响安全的因素也在不断变化,所以,安全是相对的。

第四,系统的安全观。信息安全必须是一个系统的,各因素之间协调一致的安全。防火墙,入侵检测,防病毒等等是彼此联系的,是相辅相成的。

因此,信息安全问题要受到重视,不能低估,低估会带来直接的经济和政治的损失。但是,信息安全问题也不能高估,不要因为它可能会产生严重的后果而高估它,不能防卫过当,不能为了安全就制约,甚至是阻挠电子政务的建设和发展。所以,一定要辩证地看待安全问题。

对待信息安全问题一定要非常地务实。安全不是一个虚无缥渺的、抽象的东西,它和电子政务建设息息相关,和日常的网络息息相关。从保密的角度讲,电子政务的信息安全和传统安全工作的保密原则是一样的,也需要要做到“知所必需”,即“最小权限原则”,该知道的就知道,不该知道的不知道。另外,在信息安全要做到“保所必需”,即“最低成本原则”,应该保护必须保护的那一部分内容。加强信息安全工作一定要有经济意识,如果不考虑经济效益,不考虑成本,难免会在安全上面做过头,从而带来不应有的损失。

## 六、结束语

发展电子政务的一项主要任务就是让政府在互联网上树立良好的形象。但是,如果政务系统经常遭到攻击和破坏,基本的安全都得不到保障,又从何谈起形象问题。另一个方面,由于电子政务的特殊性,一旦发生安全事故,轻则干扰人们的日常生活,重则造成巨大的经济损失,甚至威胁到国家的安全。因此,安全的意义不言而喻。失去了安全的基石,再方便、再先进的政务方式也只能是“空中楼阁”!只有切实做好信息安全工作,解决好安全问题,才能真正做到“一网管天下”,电子政务时代才会真正到来!

**参考文献:**

1 黄志澄.电子政务的内涵及发展.中国信息导报,2002

2 杨义先,林晓东,邢育森.信息安全综论.电信科学,1997(12)

3 冯杰,李会欣.我国电子政府安全运行分析.新视野,2002(5)

4 尹秀莲,于跃武.电子政务与网络信息安全.内蒙古科技与经济,2002(2)

**作者简介:**

张生霞,女,1972年生;讲师,发表论文5篇。