

11-20-2022

Studies on the Development of China's Network and Information Security

Jiwu JING

School of Cryptography, University of Chinese Academy of Sciences, Beijing 100049, China,
jwjing@ucas.ac.cn

Recommended Citation

JING, Jiwu (2022) "Studies on the Development of China's Network and Information Security," *Bulletin of Chinese Academy of Sciences (Chinese Version)*: Vol. 37 : Iss. 11 , Article 7
DOI: <https://doi.org/10.16418/j.issn.1000-3045.20221103002>
Available at: <https://bulletinofcas.researchcommons.org/journal/vol37/iss11/7>

This Scientific Focus is brought to you for free and open access by Bulletin of Chinese Academy of Sciences (Chinese Version). It has been accepted for inclusion in Bulletin of Chinese Academy of Sciences (Chinese Version) by an authorized editor of Bulletin of Chinese Academy of Sciences (Chinese Version). For more information, please contact lcyang@cashq.ac.cn, yjwen@cashq.ac.cn.

Studies on the Development of China's Network and Information Security

引用格式: 荆继武. 我国网络信息安全发展的探讨. 中国科学院院刊, 2022, 37(11): 1543-1545.

Jing J W. Studies on the development of China's network and information security. Bulletin of Chinese Academy of Sciences, 2022, 37(11): 1543-1545. (in Chinese)

我国网络信息安全发展的探讨

荆继武

中国科学院大学 密码学院 北京 100049

党的二十大报告指出, 要推进国家安全体系和能力现代化, 坚决维护国家安全和社会稳定。网络信息安全, 是国家安全体系的重要组成部分, 也是国家安全能力现代化的重要支撑; 在当今信息化时代, 其对我国政治、经济、军事及社会安全都有重要影响。在党的领导下搞好网络信息安全, 对增强国家安全能力, 提高公共安全治理水平, 完善社会治理体系都有重要意义。

1 深入理解“没有网络安全就没有国家安全”

(1) 网络信息安全成为保障经济发展的基础。信息化的快速发展改变了所有行业的运作模式, 数字化成为各行业的必由之路。所有行业, 都开始采用数字技术走向网络。银行已经将用户的资产搬到网络上; 批发零售商店已经将商品买卖搬到网络上; 人们的社交、管理、家居也快速走向网络; 政府服务人民, 让信息多跑路、群众少跑腿, 发展了“互联网+政务服务”。经济社会发展已全面转移到网络上, 形成了数字经济发展的新模式, 使得经济发展越来越依赖网络。

(2) 网络信息安全是安定生活的保障。全世界的多网融合进程已经完成, 整个世界, 包括我国民众, 都融入一张互联互通的巨大但不安全的网络中。多种终端, 包括手机、智能家居、智能汽车、监控摄像头

和移动传感器等, 以及各种业务, 包括金融、购物、科研、社交和政务等, 全部接入了一张互联互通的网络, 从而构成了新型的网络空间人类命运共同体。微信支付、工资打卡、网络购物、外卖小哥和网约车等网络应用已经成为人们生活工作的必需品。信息化时代的生活越来越依赖目前不够安全的互联网络。

(3) 网络信息安全成为政治斗争的重要阵地。随着人民生活走向网络, 意识形态的斗争主战场也逐步转移到互联网络上。网络新的信息传播方式和方法不断更新, 人工智能、“机器人水军”等成为新一代信息安全斗争的新威胁和新武器。缺乏网络信息安全的能力就很难赢得网络上的意识形态斗争。

(4) 网络信息安全成为战争胜负的决定因素。俄乌冲突充分展示了“信息战”如何成为超越“钢铁洪流”的现代化战争。计算机网络已经成为战争情报、

战争舆论、战争指挥、武器控制的重要载体，推动过去粗放型钢铁战争模式转变为精准化的信息战争模式。在信息技术高度发达的今天，面对信息化武装的新的战争形态，没有网络信息安全就不可能拥有战争的胜利。

2 发展网络信息安全需要以人民为中心

2.1 认识网络信息安全的重要性是做好网络信息安全工作的思想基础

网络信息安全并不是网络的一个具体功能，用户在使用网络的功能的时候可能并不在意其安全能力。比如，当交易系统运行稳定时，单位领导可能会想，“现在系统没有安全问题，为何还要买安全产品，为何还要花钱维护安全团队？”当交易系统崩溃时，单位领导可能也会想，“花钱维护的安全团队、买的安全产品没有用啊！”如果企业、百姓，特别是部门领导对网络信息安全不重视，我国的整体网络信息安全产业就不会有“应该有”的社会需求，我国的网络信息安全发展就会面临市场低迷的困局。“安全不能挣钱”将严重影响网络信息安全技术的可持续发展。

由于安全作为网络应用功能之外的保障，不容易形成市场价值。因此，要通过宣传和学习，让全社会了解网络信息安全的重要性，理解网络信息安全对生活、生产及科研的影响。网络信息安全可能会决定银行的资金安全、个人的信息隐私安全乃至个人的生命安全。要让更多的人明白，保护每个人的网络信息安全不仅仅是政府的责任，也是每个人、每个企业的责任。网络信息安全靠人民——只有广大民众认识到网络信息的真正价值，网络信息安全的合理市场才能形成，网络信息安全的产业才能正常发展。特别是，当前我国的网络信息安全保障能力与先进国家相比还有差距，我国网络信息安全领域的人才也存在不足的时候，网络信息安全技术的发展更加需要更多方面的了解和支持。

2.2 培养和发掘人才是网络信息安全发展的物质基础

网络信息安全是一个交叉性很强的科学技术方向，涉及很多学科，包括密码学、数学、电子学、计算机科学、物理学，甚至化学、天文学等。例如，通过能量分析能还原信息系统中的敏感数据，通过物理探测手段能获得系统的安全入口，通过化学分析能还原信息设备中的数据。正是由于其技术性高、交叉性强，网络信息安全的发展就会出现较大的不平衡和分叉，技术人才就成为网络信息安全攻防中的关键因素。

不论是网络信息安全的分析技术还是防御技术，都是矛与盾的此消彼长，都面临“道高一尺，魔高一丈”的博弈。网络信息安全市场博弈需要大量的人才队伍，因此高端人才就成为大国竞争中的决定因素。党和政府非常重视培养和发掘网络信息安全人才。更多研究机构和高校的参与和支持，培养出更多更优秀的人才，才能支撑好我国范围巨大、业务快速发展的网络信息安全事业，才能支撑国家网络信息安全尖端人才的选拔。

3 发展网络信息安全需要走中国特色社会主义道路

(1) 组织力量保障网络信息安全，应对信息技术基础不足。我国信息化发展迅速，相比而言，我国的网络信息安全基础严重不足，通用的网络信息安全技术与先进国家相比有差距。加上人们的安全意识还在不断提高中，市场需求不足，仅仅依靠自由市场经济来发展网络信息安全，我国将很难赶上先进国家的网络信息安全能力。例如，我国民间大量的信息系统是国外产品。不论是个人还是企业，可能都不愿意因为未来的危险，主动花钱替换正在运行的安全部件。同时，用户也会担心替换的安全部件有兼容性、稳定性问题，担心替换导致系统可用性的丧失。如果没有政府的投资、干预和引导，仅依靠市场，提升网络信息安全能力的安全置换就很难完成。我国的网络信息安全

全,作为国家安全的重要环节,只有依靠党的领导,依靠集中力量的优势,才能具备超越市场的发展动力,才能有规划、有步骤、有方向地实施完善。

(2) 合理使用网络信息安全人才,发挥人才更高效用。目前我国的网络信息安全人才较为缺乏,难以全面支撑我国快速的信息化发展。如果仅仅依靠市场组织,由于我国人才数量的不足,现有人才就会分散在少数企业或研究机构,很难全面服务于我国各方面的信息化发展。高效发挥现有人才的作用,全面推动我国网络安全能力的提升,仅仅依靠市场调配实现快速赶超是困难的。只有依靠党的领导,在加大人才培养的同时,通过集中力量的标准化推动,避免分散的社会重复试验,才能有效、快速推进我国的网络信息安全建设。

(3) 站在国家和人民的立场,规范企业网络信息安全要求。我国的网络信息安全事业仅仅依靠以利润为目标的企业是不够的。部分企业为了追求利润可能会略去必要的安全功能而依赖国家良好的治安形势。然而,这样的信息化建设会为国家和人民的整体安全带来隐患。在安全标准的制定中也有类似的问题——片面追求利润的企业为了减少产品研发和升级开销,一般不愿意为了明天的安全而修改和升级标准。因此,需要在党的领导下,站在人民的立场、国家的立场,统筹非市场的中立的力量,通过有效安全的标准来规范企业,推动我国的网络信息安全建设。

总之,要科学有效地做好新时代的网络信息安全工作,必须依靠党的集中统一领导,在我国的网络信

息安全发展中节约成本、用好人才、团结大众、同心同德。只有这样,我国的网络信息安全才能高高立于世界之林。

4 新一代网络信息安全技术将以密码学为基础

网络信息安全技术中,最基础和最核心的学科是密码学。特别是在互联互通的网络中,通过加密可形成解密屏障,阻挡外界对信息的解读;通过密码可表达我们的真实意愿,宣誓无法替代的操控权利;通过密码校验可保护数据,确保不被第三方修改;通过密码的数字签名,可形成不可否认的安全交易;通过同态密码,可既把计算的任务外包又不泄露数据的秘密,推动更加安全的数字合作;通过密码协议,可保护数字版权和其他数字权利。

目前,计算机安全依靠密码为基础的可信计算技术;网络访问中的传输层全面依赖以密码为主导的TLS(即SSL传输层安全协议);网络信息安全全面采用的互联网安全协议(IPSec)也是以密码为主导的;域名安全协议也依靠密码保护域名的准确性;路由安全也依赖密码保护路由信息不被篡改。

密码,能够完成他人不可知、他人不能改、来源不能伪造、持有能证明的数字处理功能。在软件定义一切、数据决定一切的未来,密码将发挥越来越重要的作用。推动和支持密码技术发展,培养和造就更多密码人才是实现我国网络强国战略,确保我国网络信息安全的一个重要的方向性工作。



荆继武 中国科学院大学密码学院院长、数据保护研究中心主任、教授,博士生导师。中国密码学会电子认证专业委员会主任,中国计算机学会计算机安全专业委员会副主任。获国家科技进步奖一等奖、二等奖等科技奖项10余项,在国际四大信息安全顶级学术会议发表论文多篇。

E-mail: jwjing@ucas.ac.cn

■责任编辑:岳凌生