中国企业报

2022/05/31

星期二

未来网络 专刊
WEILAI WANGLUO ZHUANKAN

新闻热线：13522977661
邮箱：dongjing@zqcn.com.cn

编辑：赵玲玲 校对：许舒扬 美编：王祯磊

没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济；要有高素质的网络安全和信息化人才队伍；要积极开展双边、多边的互联网国际交流合作。建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进。

——习近平主席在中央网络安全和信息化领导小组第一次会议上的讲话（2014年2月27日），《人民日报》2014年2月28日

中国自主可控产业互联网（十进制网络/FNV9）

FNV9是未来数字世界、数字货币及万物互联的安全基石

目前，在Internet技术领域，美国拥有的IPv4和IPv6地址量均位居全球第一。IPv4地址空间为32位二进制，地址空间长度设置不够，使得IP资源十分有限，到2010年已无可以分配的地址。1996年，美国互联网工程任务组（IETF）发布版本为RFC1883的IPv6，用于替代IPv4的下一代互联网协议，由于IPv4和IPv6地址格式不同，互不兼容，因此在未来很长的一段时间里，会出现IPv4和IPv6长期共存的局面。研究表明IPv6在解决IPv4地址不足问题的同时也出现了一些新的不足之处，全球IPv6技术仍处于不断研究与发展阶段。

工业和信息化部十进制网络标准工作组自2001年9月成立以来，联合国内高校和科研机构，在新一代互联网络领域进行了二十多年的研究，找到了新的网络资源“[”和“]”分隔符、256位大地址空间、以联合国国家注册代码的如“chn”等三字符国家域名、以联合国国际电信联盟如“86”作为前缀的网络地址和自治域号。提出了四层和三层混合通信模型和先验证后通信、零信任的安全机制，完成了具有中国自主知识产权的未来网络系统，获得的专利得到中国、美国、英国、俄罗斯等多个国家的认可，得到中国工信部、国家标准委等部委的大力支持，建成了除美国之外第二个网络体系。美国联邦专利局2011年通过专利US8,082,365B1授权，确认中国拥有的未来网络与美国因特网不同的网络核心技术。

国家“十四五”规划和2035年远景目标中，将未来网络纳入“国家重大科技基础设施”、“前沿科技和未来产业”（国家战略性新兴产业），要求加强网络安全防护及提升“维护政治安全能力”，要求推动联合国原则下的“网络空间国际规则”等重要建设内容。国家标准化管理委员会函[2014]46号、函[2015]49号明确工信部十进制网络标准工作组的中国专家主导制定了《信息技术–未来网络–问题陈述与要求–第2部分：命名与寻址》（ISO/IEC TR29181–2）和《信息技术–未来网络–问题陈述与要求–第5部分：安全》（ISO/IEC TR29181–5）技术报告标准。

中国自主知识产权的未来网络技术已经在山东、北京、吉林、西安、新疆、四川、江苏等地进行了测试应用，取得了良好效果。FNV9将十进制编码作为地址表示方法，具有巨大的可分配IP地址空间，是未来数字世界、数字货币、元宇宙及万物互联的基石。

未来网络的由来

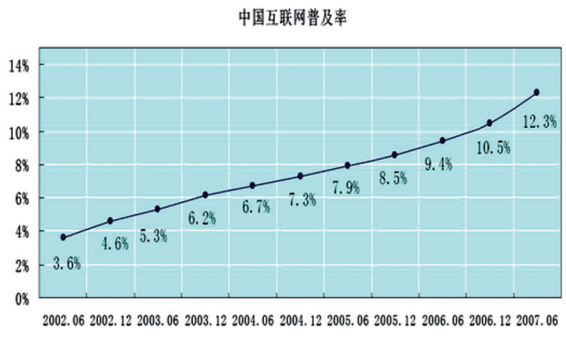
未来网络（Future Network）是一个专业名词，是自2007年以来国际标准化组织和国际电工委员会ISO/IEC（International Standard Organization / International Electro–technical Commission）推出的一个国际标准化项目，其宗旨是用空杯设计和全新架构的方法，开发一个全新的，能够独立于现有互联网之外的网络体系，实现更安全、更经济、更快捷、更灵活、更能够满足新时代要求的目标，用十五年时间研发，在2020年前后投入初步商用。

美国互联网元老大卫·克拉克（David Clark）等多位专家，2001年联名发表文章宣布，因特网的IPv6技术无法解决老旧的结构性缺陷问题，只能说明采用渐进改良路线的失败，必须坚持“空杯设计”（Clean Slate Design）的原则，不依赖现有网络的支撑，用全新思维设计全新的网络。

2005年7月，美国国家科学基金会NSF（National Science Foundation）宣布资助全球环境网络创新项目GENI（Global Environment for Networking Investigations）计划，决定用全新框架的思路研发新一代网络体系，大卫·克拉克等的文章及“空杯设计”主张是其核心的思想理论基础。这一计划没有征求美国互联网任务工作组IETF的意见，没有让IETF参与，表明新一代网络体系与互联网断然切割，确定未来网络的英文是Future Network，缩写为FN，明确显示未来网络与美国因特网没有关联、从属和延续关系。

现有的Internet网络体系下，数据安全极其脆弱

我国的Internet网络普及率不断提升。根据中国互联网络信息中心（CNNIC）公布的《第20次中国互联网络发展状况统计报告》，截至2007年6月30日，中国网民人口总数达到1.62亿，仅次于美国的2.11亿。最近半年来中国网民的增长数量更是惊人，达到了2500万，相当于平均每秒增加两个网民。



中国互联网普及率

在网络经济带动我国经济、社会整体发展的同时，我国对现有Internet网络的依赖性也越来越强，这使得我国在现有Internet网络下，经济、政治、文化和军事等方面的地位变得相当脆弱。

1.政治上，信息主权面临挑战

域名解析是打开网络之门的钥匙，是Internet网络的基础服务。根服务器更是整个域名解析系统的基础。Internet网管理者可以通过中断根服务器的域名解析服务使我国境内的Internet网络被隔绝。如果Internet网管理者授意ICANN（美国政府授权下成立的互联网名称与地址分配机构）停止根服务器对我国提供域名解析服务，那么我国境内的互联网将不能运行。2004年4月，“.ly”域名瘫痪，导致利比亚从Internet网络上消失了3天，随后据报道，原因是有两人对顶级域名管理权问题发生分歧。

少数霸权国家可以通过对根服务器实施特定的技术手段，严重干扰我国Internet网络的正常运行。它完全可以将用户对某一重要网址的访问转移到其所希望的另一个网址上，从而截取所需信息，这当然会给别国的国家安全产生巨大威胁。在Internet网络世界里，我国无法设立自主可控的Internet网络根域名服务器，没有掌握网络资源，也就没有掌握网络管理权，我国现在Internet网络的发展，实际上是向少数霸权国家控制的Internet网络租用使用权。这样，我国实际上是进入了由他国实际控制的虚拟国家疆土，在网络上发生的一切法律行为的仲裁权完全归属他国。这样，在互联网世界，国家主权不能真正独立，信息疆域也不能算真正完整。

2.经济上，代价昂贵受制于人，工业数据安全防护能力滞后

随着对网络依赖程度的增强，一方面，网络管理受制于人使得我国每年付出巨大经济支出；另一方面网络资源的有限性也将极大制约我国经济的发展。我国每年向美国支付的使用现有Internet网络的费用，包括域名注册费、解析费和信道资源费及其设备、软件的费用等，高达5000亿元以上，这个数字超过了我国目前年国防预算的数额。域名是网络生存的有限资源，让谁拥有什么域名，也就是让谁能在Internet网络上“生存”，这个最高监督权和否决权一直以来都由美国政府所掌握。美国一些大学和公司占用了大量的IP地址，如MIT、IBM和AT&T分别占用了1600多万、1700多万和1900多万个IP地址。我国获得的IP地址还不如两到三个美国大学总IP地址多。即使我国现在的Internet网络用户超过1.6亿，但域名地址的拥有量也仅有2500万，这已经制约了我国网络数字产业的发展。

此外，工业数据已成为黑客攻击的重点目标。相关数据显示，我国34%的联网工业设备存在高危漏洞，这些设备的厂商、型号、参数等信息长期遭恶意嗅探，仅在2019年上半年嗅探事件就高达5151万起，工业信息安全防护能力滞后于工业融合发展进程。

3.文化上，我国将受到严重侵蚀

在未来世界的文化之战中，谁的语言文字在网络上占主导地位，谁的文化就会在网络上获得更高的覆盖率，谁的文化就将占据统领地位。阿尔温托夫勒曾在他的《权利的转移》一书中说道：“世界已经离开了暴力与金钱控制的时代，而未来世界政治的魔方将控制在拥有强权人的手里，他们会使用手中掌握的网络控制权、信息发布权，利用英语这种强大的文化语言优势，达到暴力金钱无法征服的目的。”这就是网络时代的“文化霸权主义”。现有互联网语言运行体系的英语文化，以及网上交易和网上传播的无政府化，使得我国在文化方面受到严重侵蚀。

当今Internet网络上90%的信息是英语信息，中文信息仅占1%。语言的霸权常常意味着信息和文化的霸权。网络时代的信息霸权和强势文化的冲击使网络文化交流失去了平等交互性，变成了单向渗透。部分西方国家占据了互联网传播的制高点，向我国巨量倾销带有其政治模式、价值观念和生活方式的各类信息，以反对和消解社会主义价值观。尤其是所谓宗教文化、色情暴力文化，潜移默化地影响着受众的感受和价值判断。文化是一个民族凝聚力的重要因素，这种利用互联网实施的“文化侵略”是极其危险的，危及民族文化的独立与自存，甚至有可能动摇民族、国家的根基。

4.制网权难以确立，军事能力和军事安全遭到极大削弱

未来战场是网络空间的战场。美国著名军事预测学家詹姆斯·亚当斯在其所著的《下一场世界战争》中曾预言：“在未来的战争中，计算机本身就是武器。前线无处不在。夺取作战空间控制权的不是炮弹和子弹，而是计算机网络里流动的比特和字节……”制信息权和制网权是制空权、制陆权、制海权和制太空权的基础和核心。

（下转Z02版）