牟承晋红色文化网5 天前

长期以来，我国网络信息领域弥漫着一些奇谈怪论。例如，“中国互联网”是中国主权范围的网络，不是美国互联网（Internet）的一部分；互联网（Internet）技术是全球标准，中国已经成为 IPv6 标准化组织的主要贡献者；中国自主研发的十进制网络是“搞封闭的互联网”，不代表正能量；等等，云云。说者铮铮有词、信誓旦旦，听者云山雾罩、莫名其妙。

曾几何时，有人热衷于鼓吹 1994 年我国全面接入因特网，怎么又不敢承认中国的公众网络是因特网的一部分？依照美国的协议标准，租用美国因特网的域名地址、在美国的主权网络框架内建设的“中国互联网”，不是 Internet，难道是 Chinanet？因特网的一大推“规则”、“规矩”、“规范”，这也不许改，那也不能变，谁也不准破，究竟是因特网一直在蓄意封闭（封锁与打压）中国自主研发主权网络？还是中国的自主研发封闭了因特网？究竟是谁那么害怕中国自主研发和创建主权网络？

坚决维护国家主权、安全、发展利益，是我国坚定不移建设网络强国、数字中国的整体底线思维。主权不是简单肤浅的意识和概念，而是统筹国家发展和安全明确清晰的原则基础，是世界网络空间命运共同体的原则基础。中国的主权网络，在主权独立的基石上与美国乃至世界各国的主权独立网

络互连互通，绝不是、也不可能是美国主权网络的一部分，任何从属于他国主权网络的组成都绝不是主权独立的网络。这是大是大非。

党和国家坚持提倡、激励和扶持的自主创新，从来就是基于我国国家主权、安全、发展利益的创新，与封闭、与为他国他人的技术协议“突出贡献”扯不上任何关系。这是基本的常识、起码的道理。

必须提醒注意的是，在网信领域，任何技术协议之所以成为标准，是为了在互连、互通、互操作中规范与维护相互安全的行为。任何标准都不是也不能是固化、僵化危及和侵害他国主权、安全、发展利益的工具。

比方，物理网络（有形的硬件和软件）是人体的骨骼和肌肉，逻辑网络（包括所有的协议和数据）就是人体的神经脉络，通过自主行为人（主治医生）对数据的态势感知（基于经验积累的望闻问切），获取动态与静态信息并运筹控制（因人而异的对症诊断及实施治疗）。可见，标准和标准化行为，只是经验积累方法的传授推广，不是格式化、标本化的形而上学工具。

当今全球化信息环境（或“网络信息空间”）是一个在不断进化、深化、细化中的复杂巨系统，既有已知林林总总的组件，更有未知层出不穷的因素。正是由于“未知”因素的存在和生成，触发了建立“安全”措施的意识、制衡和对抗，

并逐步演变汇集成为“数据治理”，以及“信息优势”和“决策优势”。政治权力、经济利益和社会效应，深深地嵌入所有“安全”标准之中，无论是国际标准、国家标准还是行业、企业标准。从里到外透射“美国优先”、“美国利益至上”的协议和标准，更是如此。

二

《中国信息安全》杂志 2018 年第 1 期刊发的院士署名文章《IPv6 与网络安全》中说，现实网络开放环境中节点间的通信，更多地采用上层更为灵活的 TLS（Transport Layer Security，传输层安全）或 SSL（Secure Sockets Layer，安全套接字层）协议实现加密，与 TLS 在全世界的普遍使用相比，IPsec（Internet Protocol Security，Internet 协议安全性)的加密流量几乎可以忽略不计。因此，作者断定，“IPsec（Internet Protocol Security，Internet 协议安全性）不会成为推广 IPv6 的障碍”。

不能不严肃地指出，上述文章发表时，SSL(Secure Sockets Layer，安全套接字层）协议，2015 年就被作者推崇的美国因特网工程任务组（IETF）废弃了，文件号是 RFC 7568。作者是掩耳盗铃、自欺欺人，还是故意给国人制造科技迷雾？

TLS（Transport Layer Security，传输层安全）是在传输层与应用层之间对网络连接进行加密的一种协议，目前版本为 1.3。且不断演变，并非一成不变、固步自封。

TLS 版本	IETF 规范	发布时间	状态
SSL 3.0	-	（1996-11）	2015-6 被废弃（RFC 7568）
TLS 1.0	RFC 2246	1999-1	拟议标准（作为 SSL 3.0 的升级版，但是并不互操作）
TLS 1.1	RFC4346	2006-4	拟议标准（废弃 TLS 1.0）
TLS 1.2	RFC 5246	2008-8	拟议标准（废弃 TLS 1.1）
TLS 1.3	RFC 8446	2018-8	拟议标准（废弃 TLS 1.2）

2013 年，斯诺登披露美国国家安全局（NSA）窃听丑闻后，IETF 组织开发 TLS 版本 1.3，旨在改善与强化“美国优先”的因特网安全。从 2014 年 4 月提出 TLS 1.3 建议，到 2018 年 8 月成为拟议标准（RFC 8446），历时 4 年，修改了 28 个版本。也就是说，最后形成相对稳定适用的 TLS 1.3 版本，是在上述文章发表之后的 7 个月。作者有先见之明？还是盲人摸象？

此间，美国和世界的人权活动家（作者并不在此列）加入到 IETF，提倡将人权“固化”（Hard Coded）在网络通信协议标准中。这些重要而值得关注的问题，即技术标准是否“具有”政治性，以及协议设计在多大程度上体现或强制表现整个社会的价值，揭示了网络协议（技术标准）的实质。

尽管 IETF 解释，TLS 1.3 提供了对协商握手的加密，增强了防护数据在交换中被窃听及隐私保护的功能，有望在未

来20年或更长时间里，为因特网提供更安全、更高效的基础。尽管对 TLS 1.3 的技术分析表明，TLS 1.3 确实可以在一定程度上增强保密性和技术效率。但是，TLS 1.3 仍受到全球业界（尤其是政府网络和企业网络）的明确抵制。

上述文章发表 10 个月、TLS 1.3 最终版本出台 3 个月后的 2018 年 11 月，欧洲电信标准化协会（ETSI）发布了替代 TLS 1.3 的“中间系统安全协议”（Middlebox Security Protocol，TS 103 523-3），又被称为是行业 TLS（eTLS）。

这就是说，尽管欧洲电信标准化协会（ETSI）的 eTLS 包含（支持）IETF 的 TLS 1.3，但是在制定网络数据传输加密协议标准上，存在不同利益相关方的需求、诉求以及协议的特定保护性功能取向。

同样的道理，IPv6 作为网络互连的一个协议栈（Protocol Stack），其标准的制定和发布、采纳和遵守、部署和实施，也无可避免地存在不同利益相关方的需求和诉求。当涉及到“网络安全”，更是关系一个协议族（Protocol Suit）的问题。

基于“网络安全”的网络协议标准化，实则是人为制定一个“安全”的概念框架，并不能囊括“安全”实际发生与潜在威慑的全部和全局。认知技术标准、政治影响和社会效应之间的相互关系，主要包括三个方面不同的表现形式：

1）政治权力，把政治和权力的争夺嵌入技术标准；

2）经济利益，将不同商业（或经济）利益集团的诉求嵌入技术标准；

3）社会效应，注重和顾及与政治权力、经济利益密切相关的社会效应的叠加、递归、连锁、辐射、渗透的影响，逐步采纳和实施不断改善的技术标准。

显而易见，采纳和部署一个美国单方面制订的网络协议（如 IPv6），不可能改变其中固有的政治权力和经济利益，也不可能适应不同主权国家的特定社会效应。以解决网络地址短缺为由轻易地规模部署 IPv6，人为割裂、掩盖层出不穷潜在和不断涌现的网络安全问题，极其不负责任地交由用户放任自流、听天由命或自行消化解决，本末倒置，是非颠倒，贻害无穷。

三

据主流媒体报道,2018 年 12 月 21 日,某专家委员会的“产业发展研讨会”提出：“当前，网络的安全威胁主要是来自于设备漏洞和后门，而不是网络协议本身，网络协议是由技术标准来规范的，是全球公开的。”真是这样吗？这个说法引出三个必须正视和澄清的问题：

1）网络设备的漏洞和后门与网络协议无关吗？

2）网络协议由技术标准规范就是安全的吗？

3）我们对“全球公开”的网络协议，知之多少？

一个不争的事实是，我国的公众网络是以“全面接入”因特网即全面引进、集成、模仿、应用因特网发展而来的。对于网络协议独立自主的基础研究、系统验证和针对性创新投入甚少，追崇、迷信了几十年。所谓“免费”的网络协议、技术标准亦迷惑了我们几十年。善良的中国网民一直以为，“免费”的网络协议，即使有安全漏洞也用不着我们操心！

请问某专家委员会，究竟有几人认真读过相互依存的协议栈？又有几人仔细分析过相互关联的协议族?有几人曾有研发关键协议的努力、尝试和成果？

“网络安全”威胁和危机，被引导（甚至误导）成为仅限于约定俗成的有形硬件和软件的“漏洞和后门”，几乎完全忽视了网络通信的逻辑安全（如网络协议和数据）、行为安全（如开源情报和态势感知）以及运筹安全（如指挥和控制）。这不是一般的认识差距，而是专业知识水平和网络技术的迭代差距。

2009 年 3 月，英国伦敦经济和政治科学研究院（LSE）题为“中国与域名系统”的研究报告明确指出：“DNS 域名系统是固有政治的技术”。“固有政治”指的是因特网域名系统 DNS，其“电话簿”功能是现象，因特网域名地址的“导航”以及指挥和控制能力是本质，“美国优先”的政治元素被深嵌其中。

1982 年，美国国防部国防高级研究计划局（DARPA），资助加州大学伯克利分校的研究生开发了 DNS 软件版本 BIND；2000 年，美国国土安全部资助互联网系统联盟公司（ISC）重新开发了 DNS 软件版本 BIND 9。DNS 在因特网的协议族中是一个极其特殊的协议栈，其随着因特网的发展不断地修正和扩展。据 IETF 文档编辑统计，从 1986 年 1 月到 2020 年 10 月，IETF 发布的 DNS 相关规范性文档（RFC）共计 291 个：

RFC 文档分类	DNS 相关的 RFC 数量
标准	4
拟议标准	137
当前最佳实践	25
信息	86
实验	28
历史	10
未分类	1

另一方面，DNS 软件 BIND 又被称为是“事实上的标准”（de facto Standard），且提供开放的服务和免费下载使用。

欧洲在网络数据传输的加密协议上仍然是“当仁不让”，以欧洲电信标准化协会（ETSI）的 eTLS，替代了 IETF 的 TLS 1.3，或并存。

同样，荷兰网络实验室（NLNet Labs）在 2002 年 5 月启用了自研的权威 DNS 软件 NSD，并于 2007 年 2 月发布递归 DNS

软件 Unbound，完全替代了“固有（美国）政治”的 DNS 软件 BIND 9，或并存。

俄罗斯进行“主权互联网”断网测试演习时，一个被忽略的重要因素，是俄罗斯重要的网络门户 Yandex，在 2013 年 4 月全面（包括在独联体国家）启用了自研的 DNS 软件 yDNS，与自研的网络搜索引擎 2010-5 和网络浏览器 2012-10 结合，确保实现 90%的网络流量在本土流通，以应对来自境外的“断网”。

从欧洲和俄罗斯对网络通信协议标准的态度和行动，可见因特网及各国网络之间协议标准的“规范”和“公开”，并不能成为约束条件或形成实际束缚，也并不是完全排他的“自主可控”，关键在于所代表的“国家主权、安全、发展利益”的原则立场，以及围绕其立场产生与形成的逻辑性和系统性的风险意识。

1）在“网络安全”上的认识和方向，突出地表现于两个典型的“极端”错误悖论，即：

⑴“网络的安全威胁主要是来自于设备漏洞和后门，而不是网络协议本身”；

⑵“在 TLS/SSL 加密协议出现后，IPsec 就不再是不可替代的”，所以“IPsec 不会成为推广 IPv6 的障碍”。

上述悖论将“网络安全”简单化和片面化，既忽视忽略网络协议本身存在的“固有政治”及安全问题，又生搬硬套地

把单一网络协议（IPv6）的互连性作为网络安全能力人为地强化与夸大。上述悖论在国内网络安全产业界造成相当大的逆向影响和差距，迫使用户一味“委身”求全，各种“马甲”成风。

2）网络协议是基础性技术，既有历史的沿革，又有发展的创新。对标美国、欧洲、俄罗斯，我国网络信息领域关键的缺失和差距，在于基础性研究和积累严重匮乏，概念和理念上的转型及定义和定位严重滞后。

3）总书记“没有网络安全就没有国家安全”的论述，清楚地指出了“国家安全”标准化框架主要由三个宏观要素构成，即：政治权力，经济利益，社会效应。或可概括为“国家主权、安全、发展利益”。这三个要素也是主导各国制定“标准化协议”的三个原驱动力。

对于坚定不移建设网络强国、数字中国的中国党政军民来说，应当充分、深刻地认识“技术不是中立的”重要性，彻底打破思想上、意志上、行动上的自我封闭，开创冲破美国技术封闭壁垒的自主创新发展新格局，坚决维护国家主权、安全、发展利益，在当前的全球性网信安全斗争中，举国协力、同心同德“发扬斗争精神，树立底线思维，准确识变、科学应变、主动求变，善于在危机中育先机、于变局中开新局，抓住机遇，应对挑战，趋利避害，奋勇前进。”

（本文感谢邱实提供技术资料、给予技术指导。2020 年 11 月 27 日完稿）