【编者按】近日，新华社高级编辑杨兆波加按语，在今日头条“舆情智库”发表了《牟承晋：预判风险是防范风险的前提，把握风险走向是为谋战略主动》一文。

按语指出：著名信息安全专家牟承晋，在和有关部门舆情与信息安全课题组负责人杨兆波先生沟通与交流时指出，科学是验证和试错的过程，严格地说，验证即证伪，试错是为了纠偏。几十年来，某些既得利益者编织的反科学樊笼，严重禁锢了我国网信领域自主创新的思想、意志和行动。尤其是涉及重大的网络信息安全问题，有些观点公然悖逆科学常识，即便一二十年的实践证明过犹不及的事实俱在，也没有引起高度重视。国内针对

基础设施、关键技术自主创新提出和研发的协议、标准、见解、发明， 有的是长期得不到科学实验和验证的公开、 公正、公平的呵护、扶持、法治保护和资源保障。这件事不能不发令人深思。以下是牟承晋先生的观点。具有重要参考价值。（新华社高级编辑 杨兆波）

为此，昆仑策网和本院公众号经作者授权，将原稿全文编发如下，以飨读者。

科学是验证和试错的过程，严格地说，验证即证伪，试错是为了纠偏。
几十年来，我国网信领域不经过科学验证，或者验证缺乏科学态度走过场，甚至时间空间反复验证充分证伪也不纠错，凭空想象、猜测、臆断、捏合，不负责任胡乱结论、讳疾忌医的事情经常发生。
某些既得利益者编织的反科学樊笼，严重禁锢了我国网信领域自主创新的思想、意志和行动。尤其是涉及重大的网络信息安全问题，公然悖逆科学常识的错谬大行其事，即便一二十年的实践证明过犹不及的事实俱在，也不予矫枉过正。国内针对基础设施、关键技术自主创新提出和研发的协议、标准、见解、发明，一再横遭打击、冷漠、压制，长期得不到科学实验和验证的公开、公正、公平的舆论呵护、政府扶持、法治保护和资源保障。不能不发人深省。

一、“镜像”替代“根域名”的谬论必须澄清

镜像服务器可以替代根域名服务器的说法，时下又在网上网下活跃起来。有人以此论证因特网“断网”不可能发生，“断网”对我国网络运营和服务不会有影响。“镜花水月”的说道，竟然铮铮有词地成了因特网的“科学论断”？
因特网的域名系统（简称 DNS），是通过一系列复杂运算组合其指定的域名、IP 地址和自治域，适应与支撑不断演变的应用功能最基础、核心的数字化系统。其中包括：

——通信协议的关联规范（美国因特网工程任务组 IETF 至 2020 年 10 月共计发布了 291 个 RFC 文件）；

——注册域名和分配的地址组成的数字化空间；

——根域名、顶级域名、权威通用域名层次化服务的体系结构；

——基础软件定位及实施指挥与控制(自主研发专用,或开源“免费”使用)。

显而易见，虽然“根域名”重要，但仅仅是因特网中构成数字化系统的一个子系统。“镜像”根域名，不可能是照了张“全家福”，也绝不可能反射或反应层次化服务体系结构的全部运转和运行真相。以偏概全，一叶障目，向来是哲学与科学的大忌，是反哲学、逆科学的一贯伎俩。

换句话说，作为子系统的“根域名”即便是被“镜像替代”，也不可能规避、防止其它关联子系统被攻击或被限制，整个域名解析系统（DNS）停服或断网仍然不可避免，仍然只能是不堪一击的“马其诺防线”。

如果建几个“镜像服务器”就可以轻而易举地替代“根域名”子系统，黑客们完全有理由和动机在因特网中建上多个虚假、另类的“根域名”子系统“搅得周天寒彻”，何必还整天钻漏洞、设木马、放病毒呢？为什么“不”呢？是不能，还是不可能？还是能也不能？

“镜像替代”论者从一开始，就将美国为实验和验证 IPv6 可操作性提出的“雪人计划”，编造成自主创新“镜像替代”的故事，为了自圆其说不断地撒谎，甚至拉帮结派地撒谎。“带头大哥”说，美国因特网在欧洲的根服务器有一个在英国，于是乎，主流媒体、著名高校、科研机构、专家学者以讹传讹，多少年来都异口同声地咬定英国有因特网的根域名服务器。事实是，13 个“根域名服务器”系统有一个在荷兰、一个在瑞典，30 多年从未改变过，公开信息，稍微查一下就明了。盲目崇信“权威”、“教授”不科学、不严谨麻木如此，不严肃、不负责荒谬这般，可见我国网信樊笼害人匪浅。

还有多少这样愚弄我国网民、网信从业人士、主政网信官员的事情和是非，真应该好好查查、清清、算算！

二、“盲人摸象”式地“创新”研发必须扭转

科学道路上没有捷径。有人提出“通过镜像顶级域名的数据，作为根域名镜像方案的缺失互补和顶级域名被停服的备份”，自我标榜地称之为“拍案叫绝的”创新。实际上，掩盖了缺乏核心协议基础研发的安全隐患，套上哗众取宠的“马甲”掩耳盗铃，在错误的方向和道路上渐行渐远。

1）根据中国信息通信研究院的报告（信通院 2020-6），截至 2019 年 12 月，我国域名注册市场规模为 5,108.8 万个，其中，国家顶级域“.CN”域名 2,300 万个；“.COM”域名 1,566 万个；合计占我国域名市场的 75.7%。活跃域名数量分布：

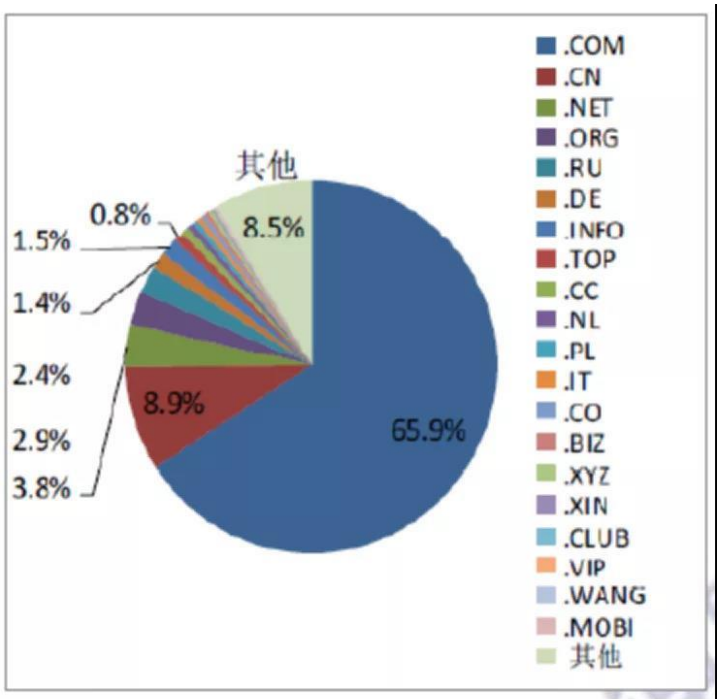

图 1 我国活跃域名数量 TOP20 的顶级域份额
（来源：信通院）

图 1 可见，我国活跃域名的解析超过 91%依赖于境外服务。是境内网信樊笼锁住了境内的自主服务，还是境外网信樊笼关闭了境内的自主服务？还是境内境外联合构成了封杀封闭我国境内域名解析自主创新的网信樊笼？

2）根据对全球互联网（Internet）公共（递归）域名服务器的监测统计，截至 2020 年 12 月 4 日，中国大陆拥有公共域名服务器（仅仅是 53 端口/UDP）的数量为 776,618 台，占全球总数的 39.97%。请注意，这是在动态变化的数量，例如，10 月 22 日的数量为 1,106,552 台，占全球总数的 46.18%。

那么，是谁以及为谁提供公共的 DNS 服务？作为域名空间入口的递归域名解析服务，在我国处于良莠不齐的混沌境地，安全监管严重缺失。这是不是长期盘根错节的网信樊笼所致？

3）内容分发网络（简称 CDN，又被称为是“加速”网），正在被大量普遍地针对性应用于中国的网络信息领域，方兴未艾。CDN 是叠加在传统网络基础设施上的虚拟网，借助于 DNS 实现用户定位（负载均衡）重定向，即选择（确定）终端用户与业务服务之间的最佳匹配（如最短响应时间及路径）。

其中一个典型的隐性特点是，通过传统的域名解析，数据不再映射到 IP 地址，而是转换（旋转）到预设置的域名“别名”（简称 CNAME），进而不透明地实现对业务和应用（包括数据流）指挥与控制的实时动态转移（或曰时空迁移）。

例如，美国驻中国大使馆（其各领事馆也是相同模式），以顶级域名“.CN”注册了其权威域名。在实际应用时，通过“别名”（CNAME）实时转移（旋转）到美国 Akamai 公司在美国境内的托管服务：

美国驻华大使馆的域名	缓存时间（TTL：秒）	类型	服务响应结果
china.usembassy-china.**org.cn**	600	CNAME	cert5.state.gov.edgekey.net
cert5.state.gov.edgekey.net	300	CNAME	e4517.dscx.akamaiedge.net
e4517.dscx.akamaiedge.net	20	A	23.66.67.233（IPv4 地址）

传统域名解析服务模式被 CNAME 实时旋转模式颠覆，似乎是“神不知鬼不觉”，如何能够镜像？又如何能够实现“镜像替代”？这究竟是谁针对谁的“拍案叫绝”？

试图“以顶级域名的镜像应对顶级域名的停服”，还必须兼顾对域名空间入口（递归服务）的信息同步，小范围也许可以做到，在全国全网是不可能实现的。这种一厢情愿臆想臆断地“盲人摸象”，也许是对网信樊笼的一种下意识地挣扎，却只能是毫无科学力量支撑地徒劳。

三、美国对我断网停服的技术必然性不可否认

“镜像替代”论者断言，“互联网（Internet）的‘DNS 根服务器’不是‘核按钮’”。曾几何时，多家媒体大加渲染这个“正确答案”。

因特网应用中，有一个专用术语是“终止开关”（Kill Switch），即在紧急情况下关闭所控制的网络或服务的安全功能。这就像是家家户户那个“总电门”。这也是因特网的常识。

2016 年 7 月 12 日，美国因特网域名与数字分配机构 ICANN 发表官方博文，题为：“何谓互联网（Internet）终止开关？谁有钥匙（密码）？”文中回答，域名根的解析服务需要加密验证，由 ICANN 负责，所运用的先进技术是 KSK（密钥签名密钥），也是互联网（Internet）的钥匙。宣示了因特网“终止开关”的存在。ICANN 自 2019 年以来连续两年部署和实施“DNS 执行日”（DNS Flag Day），为“无缝地过渡到未来 30 年 DNS 时代”奠定基础。

上世纪九十年代（或更早），美国国家安全局（NSA）就已经提出和实践在网络信息环境攻防的“武器化”。目前仍在使用的“X Key Score”网络监听工具，业内称为“敲响 DNS 丧钟”的“悠悠牛铃声”（More Cow Bell）等，都是典型的“武器化”工具和手段，主要依托于被预置在硬件和软件及通信协议中的后门及暗桩。2020 年 9 月 30 日，美国国防部发布“数据战略”，强调数据“武器系统”，正式拉开抢占“信息优势”和“决策优势”的帷幕。

DNS 既具有网络通信“电话簿”作用，更是类似于“北斗”和 GPS 的因特网“定位”系统，以及指挥和控制中枢。在 DNS 近 40 年沿革和发展的历史中，可见三个主要阶

图2 DNS发展和沿革中的三个主要阶段

段：

上述“正确答案”，显然是沉浸（或停留在）上世纪九十年代的惯性思维不思进取，对某些专家和国人的思想、意志和行为的误导，是我国网信樊笼深度阻遏与羁绊的表现。

终止开关是美国 ICANN 明示的因特网最关键、最核心、最深或最高层次严密控制的“暗桩”，是可以瞬间指向因特网覆盖的任一区域性、局域性、行业性、专业性范畴令其断网停服（瘫痪网络）的控制中心。因特网的“终止开关”就是“核按钮”，一旦启动，必然会对我国政治经济社会发展产生影响深远的巨大综合破坏力。否认因特网“终止开关”的“核按钮”性质与功能，不是什么技术创新，更不是什么“大义凛然”，而是蓄意掩饰“帝国主义亡我之心不死”的真相，是麻痹我们心智、束缚我们手脚的别有用心。

习近平总书记告诫全党全军和全国人民，“没有意识到风险是最大的风险。”预判风险所在是防范风险的前提，把握风险走向是谋求战略主动的关键。

久在樊笼里，复得返自然。坚定不移地建设网络强国、数字中国，坚持维护国家主权、安全、发展利益，全党全军全国人民同心同德，顽强奋斗，自力更生，自主创新，一定能够全面开创我国网信领域的新时代、新征程、新发展格局。

【感谢邱实对本文提供的技术指导。本文完稿于 2020 年 12 月 7 日。】

（作者系中国移动通信联合会国际战略研究中心主任，昆仑策研究院高级研究员，浙江省北斗未来网际网络空间研究院首席研究员；

来源：昆仑策网【**原创**】，全文稿）