# 耸人听闻的“后门”？——美国《安全设备法》简评

作者：潘永建 | 黄文捷 | 左嘉玮

美国当地时间 11 月 11 日，美国总统乔·拜登签署了《安全设备法》(Secure Equipment Act)，该法将阻止联邦通信委员会(“FCC”)向被视为“安全威胁”的公司发放电信设备许可证。业界认为，该法是针对华为、中兴等中国科技企业的最新贸易限制措施。通过本文，通力合规团队将简要解读《安全设备法》的来龙去脉及对相关企业带来的影响。

## 一. 《安全设备法》的背景

美国是世界上数字化连接最紧密的国家之一，13 台互联网根域名服务器中有 10 台坐落于美国，因此美国高度重视对于信息基础设施的安全防护，并将其网络安全视为“国家安全”的重要组成部分。在这种背景下，中国、俄罗斯等网络大国被视为严重的威胁，因为其有能力实施网络攻击而造成严重的损失。

2012 年，美国众议院特别情报委员会曾发布一份《由中国电信公司华为和中兴通讯带来的美国国家安全问题》报告(“PSC 报告”)[1]，指责华为和中兴的设备存在安全隐患，其主要理由是中国政府有可能强迫这两家企业在其电信设备或系统中植入“恶意硬件或软件”，从而对美国的信息关键基础设施构成威胁。PSC 报告指出，美国政府部门不应该继续使用华为或中兴的设备，同时呼吁美国私营电信公司选择其他的供应商。

2019 年，美国通过了《安全和可信通信网络法案》(Secure and Trusted Communications Networks Act)，以保护美国的通信供应链免受来自外国供应商的安全威胁。该法案要求 FCC 制定一份“对美国构成国家安全威胁”的“受限设备与服务清

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

[1] M Rogers and D Ruppersberger, 'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE'

单”(List of Equipment and Services Covered By Section 2 of The Secure Networks Act)，将清单中所列设备称为“受限通信设备或服务”，禁止美国电信运营商使用联邦补贴“购买、租用、租赁或以其他方式获得受限通信设备或服务。[2]2021 年 3 月，根据该法案，FCC 宣布将华为、中兴、海能达、海康威视和浙江大华 5 家中国企业生产的通信和监控设备列入了受限设备与服务清单[3]。

2021 年，美国通过了《安全设备法》，要求 FCC 通过新的规则(“FCC 新规”)，明确 FCC 将不再审查或批准任何对国家安全构成威胁的设备或服务的授权申请。[4]

## 二. 《安全设备法》的影响

2019 年的《安全和可信通信网络法案》仅禁止美国企业利用联邦补贴“购买、租用、租赁或以其他方式获得”受限通信设备或服务，如果资金来源不涉及联邦补贴，则不受限制。最新的《安全设备法》对华为、中兴等公司的受限通信设备或服务施加了更加严格的限制。

根据《安全设备法》，FCC 应在该法生效后 1 年内通过 FCC 新规，新规应包含以下内容:

(1) FCC 于今年 6 月发布的拟议规则[5]中规定的程序，其中包括：任何受限通信设备或服务必须经过认证程序(certification process，需 FCC 的批准或授权)获得设备授权;
(2) 规定 FCC 不得审查或批准任何受限通信设备或服务。

这意味着，将来美国私营企业无论是否接受政府资助均不得新购入或以其他方式获得华为、中兴等公司的受限通信设备或服务。

## 三. 卡巴斯基诉美国国土安全部案[6]

中国企业并非美国政府的唯一怀疑对象，俄罗斯网络安全公司卡巴斯基此前遭遇了类似的禁令。2017 年 9 月，由于担心俄罗斯政府可能会利用卡巴斯基对美国联邦信息系统的访问权限进行恶意操作[7]，美国国土安全部指示联邦机构在 90 天内删除已使用的卡巴斯基产品。随后，美国国会通过了正式禁令，决定禁止联邦政府使用卡巴斯基的任何硬件、软件或服务。卡巴斯基提起诉讼，认为这一禁令违反了美国宪法的“禁止剥夺公权”条款——”不得制定公民权利剥夺法案或追溯既往的法律(No bill of attainder or ex post facto law shall be passed)”，即禁止国会在未经审判的情形下，以立法的形式对一方进行惩罚。

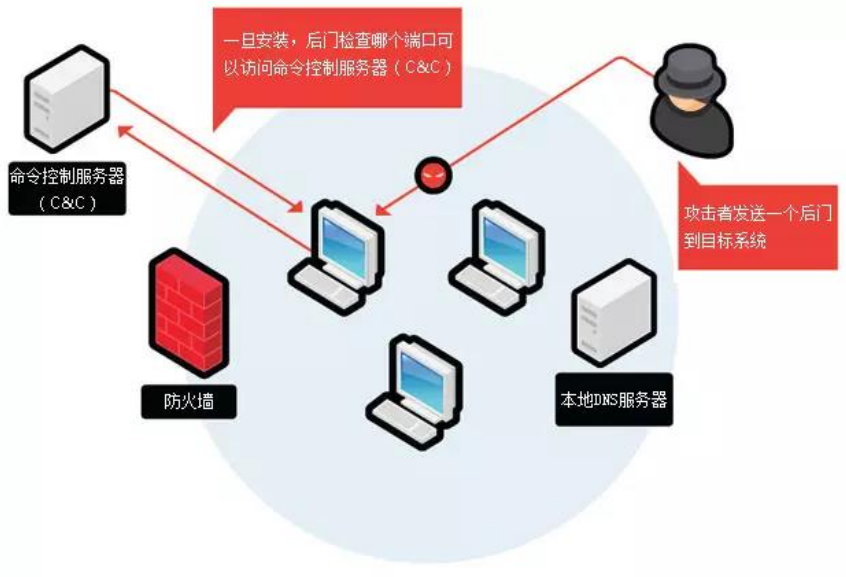
[2] Secure and Trusted Communications Networks Act. SEC.3.(a)(1)
[3] 详见 https://www.fcc.gov/supplychain/coveredlist，最后访问日期: 2021 年 11 月 16 日
[4] Secure Equipment Act. SEC.2.(a)(2)
[5] Notice of Proposed Rulemaking in the matter of Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program
[6] Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec. , 909 F.3d 446, 457 (D.C. Cir. 2018)
[7] 在美国国会的听证会中，专家解释道: “无论卡巴斯基是否愿意合作，俄罗斯政府都可以利用卡巴斯基产品作为后门进入联邦信息系统。”

美国哥伦比亚特区巡回上诉法院认为，考虑到卡巴斯基的产品威胁美国联邦信息系统的可能性并非微不足道，以及这种入侵可能造成的危害将十分严重，国会决定停用卡巴斯基的产品是一个合理和平衡(a reasonable and balanced)的回应。法院同时指出，尽管禁令可能会给卡巴斯基带来沉重的损失，但是“制裁的严重程度并不能决定其性质”，因此国会的禁令不是在未经审判的情形下对卡巴斯基施加惩罚，而是采取保护联邦信息系统免受俄罗斯网络威胁所必需的预防措施。法院最终认定国会没有违反美国宪法，驳回了卡巴斯基的上诉。

## 四. 何为“后门”

在种种禁售事件中，美国政府最为普遍的一种担心是，(尽管没有证据存在真正的威胁)华为、卡巴斯基等他国企业有可能受政府指使在设备或软件中植入“后门”，从而秘密地入侵美国电信网络。那么，经常被提起的后门到底为何物?

在信息安全领域，后门(backdoor)通常指代一种可以绕过安全性控制而获取系统或程序访问权限的机制。通过后门，攻击者可以在未经用户知情或许可的情形下访问其设备，或者获得加密系统中的原始明文。例如：某些版本的 Windows 系统在登陆时可以通过组合键 Win+U 调用“放大镜”程序，辅助视力有障碍的用户进行操作，黑客在使用同名的 magnify.exe 替换原始的放大镜程序之后，可以通过运行它绕过系统登录验证。




图源：亚信安全

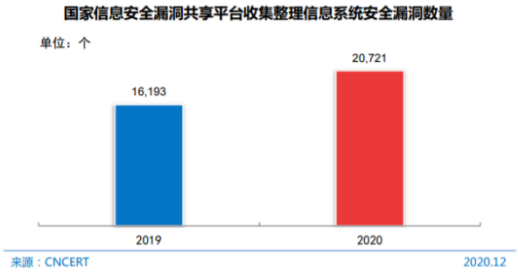
如图，后门就像一个进入用户电脑的秘密入口，通过它可以绕开防火墙等安全机制(前门)。

### 后门与漏洞

一个经常与后门同时提起的术语是漏洞(vulnerability)，漏洞与后门均指计算机系统安全方面的缺陷，攻击者也可以利用产品已有的漏洞植入自己的后门。两者的主要区别在于，后门通常是信息产品/服

务提供商或黑客故意设置的，而漏洞通常是提供商由于技术水平或安全意识不足而未能及时发现的安全问题。实务中，往往难以区分企业在主观上是“故意”还是“过失”，看似无意的代码漏洞也有可能是提供商精心预留的后门。

后门/漏洞是网络安全面临的主要威胁之一，中国国家互联网应急中心(“CNCERT”)数据显示，去年共监测发现我国境内被植入后门的网站为 61948 个，国家信息安全漏洞共享平台收集整理的信息系统安全漏洞为 20721 个。[8]


**后门分类**

后门(广义上的)不一定带有非法目的，如果具有正当理由，政府或硬件/软件提供商可以在产品中预留合法的技术干预措施。或者说，法律禁止的是设置隐蔽的恶意程序(狭义上的后门)，在事前已经合法披露的措施不应理解为一种后门。

**合法“后门”**

合法监听(Lawful Interception)：合法监听主要用于打击犯罪，保护国家、公共安全。虽然未直接使用“后门”这一术语，但是各国法律通常会要求通信服务提供商(Communications Service Provider, CSP)为执法机构监听或侦查犯罪活动提供技术支持。

国际通信标准化组织 3GPP SA3 工作组将在 5G 技术标准中定义了合法监听功能——”由通信服务提供商采取的合法行动，包括提供特定目标身份，隔离目标通信，并将通信副本发送给执法部门。”[9]根据这一标准，执法部门在拥有合法授权的前提下，可要求 CSP 配合拦截特定目标(通常是犯罪分子)的通信。而对于加密的通信服务，如果要提供拦截功能，服务提供者必须设计某种机制(后门)使其能够访问未加密的通信数据。

技术支持：常见于工业设备的信息控制系统，此类系统一般较为复杂，因此提供商会为其服务/设备预设远程访问功能，旨在借此实现维护调试、补丁升级、bug 修复以及收集产品使用信息等功能。如果已经事先明确地告知用户并活动同意，此种“后门”通常亦在法律允许的范围内。

[8] CNNIC：第 47 次《中国互联网络发展状况统计报告》
[9] 3GPP TS 33.126 definitions

**恶意后门**

即用于非法获取信息系统访问权限的后门。

攻击者通常通过恶意软件(蠕虫或者木马等)在用户的设备中安装后门，并将其伪装为合法程序，从而在无形中监视用户的活动，窃取用户的数据。后门也可以隐藏在硬件/固件之中，例如在芯片制造时设计一些具有后门功能的逻辑电路，在被激活后能够使攻击者绕过硬件的安全防护机制。

令人担心的是，合法后门与恶意后门之间并非泾渭分明，为执法部门设置的后门很可能会被恶意攻击者劫持，给用户带来额外的安全风险。例如，2017 年，美国国家安全局泄露了 Windows 操作系统多个版本的漏洞，黑客随后利用这一漏洞传播“Wannacry”勒索病毒，造成全球近百个国家遭受大规模网络攻击。此外，企业或其员工也可能出于自身利益滥用后门(例如，用于非法收集用户信息)。

## 五. 结语

美国政府无法完全禁止后门。事实上，以美国为首的五眼联盟近年来一直在呼吁科技企业向政府与情报机构提供加密“后门”。因此，《安全设备法》对于华为等公司的限制措施可能更多的是出于对中国政府以及中国科技公司的不信任。依据“卡巴斯基案”这一先例，美国法院似乎认为，在仅有理论安全风险的情形下(出于地缘政治和商业因素，这些风险往往被夸大了)，国会就有权禁止使用他国企业的产品和服务。可以理解的是,美国政府可能对他国企业的产品存在“合理”的安全担忧(精心设计的后门很难被检测出来，因为它们看起来与正常的代码和电路别无二致)，但相比起“卡巴斯基案”中法院在论证国会禁令的“合理性”时所强调的——“联邦政府只停止使用自己的卡巴斯基产品，所有其他个人和公司仍然可以自由购买和使用卡巴斯基产品”，最新的《安全设备法》全面禁止华为等公司产品的反应是否已经超出了必要的限度?《安全设备法》是否会引发中国按照《网络安全审查办法》等法规对美进行反制？我们将拭目以待，持续关注。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

| 上海 | 北京 | 深圳 |
| --- | --- | --- |
| 上海市银城中路 68 号<br>时代金融中心 19 楼<br>T: +86 21 3135 8666<br>F: +86 21 3135 8600 | 北京市建国门北大街 8 号<br>华润大厦 4 楼<br>T: +86 10 8519 2266<br>F: +86 10 8519 2929 | 深圳市南山区科苑南路 2666 号<br>中国华润大厦 18 楼<br>T: +86 755 3391 7666<br>F: +86 755 3391 7668 |
| 香港 | 伦敦 | |
| 香港中环遮打道 18 号<br>历山大厦 32 楼 3201 室<br>T: +852 2592 1978<br>F: +852 2868 0883 | 1/F, 3 More London Riverside<br>London SE1 2RE<br>T: +44 (0)20 3283 4337<br>D: +44 (0)20 3283 4323 | |

**www.llinkslaw.com**

**Wechat: LlinksLaw**

**本土化资源 国际化视野**