微软“甩锅”背后的野心与国家安全问题

7月19日，网络安全公司CrowdStrike在推出软件更新时，没有经过严密测试就大规模推送，导致许多微软视窗用户蓝屏死机，微软云服务也连带崩溃。随之而来的是全球大范围的网络故障，波及欧美、亚洲多国的航空、医疗、金融、零售等多个行业，造成的负面影响和冲击震惊全球。微软发言人表示，2009年在欧盟委员会的坚持下与其达成了一项协议。正是这一决定增加了系统出错的可能性，未来不可避免地会再发生类似的大规模技术事故。面对微软的强烈指责，7月23日，欧委会发言人驳回了微软的指控，并表示，“该事件并不局限于欧盟，微软在事件发生前后从未向委员会提出过任何有关安全的担忧。”

7月19日，全球许多采用微软产品的系统在这一天“蓝屏死机”，大瘫痪。

没有网络安全就没有国家安全习近平总书记指出，“没有网络安全就没有国家安全”，凸显了我国网络安全保障的重要性。这一场由美国网络安全公司CrowdStrike的软件更新引发的全球IT大瘫痪事件导致多个国家和地区的航班系统、银行系统、超市系统等众多行业受到严重影响，运行微软视窗操作系统的电脑陆续出现蓝屏、访问异常等问题。对于一个国家来说，过度依赖某一家公司或少数供应商的操作系统和安全软件可能会带来潜在的安全隐患。

从国家安全的角度来看，这种大规模的IT故障可能会被不法分子或恶意组织利用，对国家的政治、经济、社会等方面造成更严重的危害。首先，在政治领域，网络已成为各国政府进行信息传播、政策发布和民意收集的重要渠道。一旦网络安全出现漏洞，敌对势力可能会利用这些漏洞进行虚假信息传播、恶意舆论引导，从而破坏国家的政治稳定和社会秩序。其次，在经济方面，国家的金融系统、能源供应、交通运输等关键基础设施都高度依赖网络。网络攻击可能导致金融市场动荡、能源供应中断、交通瘫痪等严重后果，给国家经济带来巨大冲击。再者，军事领域的网络安全更是至关重要。现代战争已经从传统的战场延伸到了网络空间，军事指挥系统、武器装备控制系统等都可能成为网络攻击的目标。一旦网络安全防线被突破，国家的军事机密可能泄露，军事行动可能受到干扰，直接威胁到国家的安全和主权。

微软“甩锅”背后暴露了什么野心？

微软发言人将此事的责任归咎于欧盟，微软希望摆脱欧盟的束缚，不再给任何第三方安全软件访问系统底层的权限，但这样直接的后果就是所有的第三方安全公司都会“死掉”，微软的目的是垄断操作系统底层安全软件的权益。

假设没有欧盟的政策限制，那么意味着微软只要垄断其操作系统，就不会有任何第三方独立的安全软件存在。这一点对中国意味着国家安全的灾难，如果第三方软件都被微软取消了访问系统底层的权利，那么在中国电脑里发生了什么就只有微软才能知道，而微软是不可能把某些国家的情报机构或者网军在中国的攻击行为告诉中国政府，那么就意味着中国失去了对整个网络安全态势的感知和把握能力，也意味着其他国家的网络攻击者在中国可以继续大行其道，形成单向透明的优势，那将是中国网络安全彻底的失守。在这种情况下，若中国的大部分电脑还是在用Windows操作系统，那么在这些系统里某些国家网络攻击者的攻击软件可以在掩护下想干什么就干什么，这对于我们整个国家网络安全、信息基础设施、包括城市基础设施形成重大的威胁。

微软“瘫”局下中国的“安然”与未雨绸缪

微软全球IT大瘫痪事件在全球范围内引发了巨大的混乱，但令人意外的是，多数中国企业得以幸免。其中一个重要原因是，中国企业近年来对自主研发和技术创新的重视程度不断提高。许多企业已经逐渐减少对国外技术的完全依赖，拥有了自己相对独立和稳定的技术体系。另外，中国在

网络安全和数据管理方面的严格监管也发挥了作用。相关法规要求企业必须具备一定的应急和数据保护能力，这使得中国企业在面对此类全球性危机时，有更充分的准备。

尽管此次多数中国企业在微软全球IT大瘫痪事件中幸免于难，但微软此次事故提醒我们，网络安全威胁具有全球性、无国界性和隐蔽性的特点。一个国家的网络安全问题不仅可能源于内部的技术漏洞和管理疏忽，也可能受到来自外部的恶意攻击和网络犯罪的威胁。因此，保障网络安全需要国家从战略高度出发，建立健全的网络安全法律法规体系，加强网络安全技术研发和人才培养，增强全民的网络安全意识。