网络战争该进攻还是防守？思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_BD_91_E7_BB_9C_E6_88_98_E4_c101_644078.htm Conficker蠕虫病毒已经感染了成千上万的计算机系统，网络安全专家们开始担心更深层次的僵尸网络攻击。 要求解决这个最新威胁的呼声越来越高，两名德国研究人员Felix Leder和Tillmann Werner(Bonn大学的学生)倡议在最新威胁用于其他目的时，提前制止僵尸网络的产生。“ 目前大多数解决方法都是响应式的，当攻击发生后才开始采取行动，”Werner在网络战争会议上表示，“ 我们应该提前制止这种攻击。”这两名学生是很有名的安全研究人员，三月份时，他们发现了一种使用网络扫描检测感染Conficker计算机的方法，这种方法可以检测和移除大量受感染主机。在他们的最新研究中，Leder和Werner主要关注四种复杂僵尸网络：Conficker、Waledac、Storm和Kraken，他们表示他们已经非常了解这些僵尸网络攻击和解除恶意网络的方法。 参加网络战争会议讨论的两名美国政府官员认为，美国需要采取强硬政策允许在网络空间开展进攻战略，但这两名官员都不愿意透露其名字和机构。美国和其他国家如果采取积极的网络攻势，将有能力打击网络罪犯的攻击。“ 我们似乎可以发展网络能力来提高整个军事态势，有时候必须采取进攻方式来保护安全。”美国国家研究理事会研究主任Lin Herbert表示。 虽然围绕网络攻击能力的政策仍然不成熟，但这些技术将为政策制定者带来更多选择。如果国家开发出压倒性的网络攻击技术，就能够带来数字版“ 核缓和 ”的效果，印度国防部的国防研究与发展阻

止的科学家Amit Sharma表示。但是也有人持反对意见，他们认为当你不知道网络空间的攻击幕后策划者是谁时，很难发动进攻。只有假设在最好的情况下，我们才能够真正打击发动攻击的幕后黑手，而实际上几乎每次都发现我们在攻击无辜用户的被感染的计算机。即使“攻击”其实是个软件补丁或者移除恶意代码的程序，还是可能发生错误。在真实案例bot软件感染处理关键数据或者控制医疗系统和关键基础设施的计算机中，真正令人担心的问题是，修复系统可能会导致机器崩溃。法律和赔偿责任方面的担忧阻碍了研究人员的脚步，如来自波恩大学的Leder和Werner试图采取先发制人的方法来打击僵尸网络攻击，研究人员认为这些担忧是错误的。“在现实中，我们看到过医疗设备中的恶意软件让这些设备无法运行，”Leder表示，“可能在将来恶意软件真的可能害死人，虽然现在没有发生，因此，采取积极的先发制人的方法可以预防这些问题。”