M.Phil Year 2 Supplementary Reading 13TT Week 2

美制定网络战争守则 可入侵外国电脑种病毒

美国五角大楼制定了一份网络武器和工具清单，其中包括能破坏对手重要网络的电脑病毒，这份清单对美国如何开展网络战争提供了依据。

“病毒”武器跃出水面

不愿透露姓名的美国军方官员称，保密的网络武器清单在数月前已投入使用，并已得到美国中情局等机构的认可。这份清单中包括了一些经五角大楼批准的武器，可在对敌作战中使用。

一名高级军方官员表示：“不管是坦克、M-16 步枪还是电脑病毒，我们都得知道如何使用，何时能够使用，什么能用以及什么不能用。”该官员称，将网络武器整合成一份正式的功能清单，或许是近年来美国军方网络政策中最重要的进步。

网络打击需总统授权

例如，这份清单表明，军方需要总统的授权才能入侵外国电脑网络、留下日后可激活的病毒。但如果军方入侵外国电脑网络开展一些其他活动时，则不需要经过总统的授权，这些活动包括研究对手的网络袭击能力、检查供电站或其他机构的运作方式。美国军方网络军队还可以不经总统授权为日后病毒袭击做下标记。

在这一网络武器使用框架之下，任何网络武器的使用都必须与受到的威胁成正比，不能造成不必要的附带损坏，避免对无辜民众的伤害。

美国军方高级官员透露，根据这份清单，在敌对区域以外或美国不处于战争状态时使用任何网络武器，都被称为“直接行动”，需要得到总统的批准。

网络武器分 3 个等级

这份清单将武器的使用分为 3 个等级：全球、区域和敌对地区。全球范围内的行动属最高等级行动，行动的附带后果最难以预测。

五角大楼制定这份清单的原因之一是，在网络中决定何时回击比在传统战场上更为困难和复杂，目标可能包括位于不同国家和地区的电脑。

一些法律专家建议，制定法律以肯定国防部长拥有在某些条件下“在网络中开展秘密行动”的权力，这些行动必须是支持打击恐怖分子的行动。起草这一法规的众议院军事委员会副主席马克·索恩伯里称，之所以起草这一法律，是因为在伊拉克和阿富汗战场上的指挥官们非常苦恼，一些针对美国军队的袭击是敌方通过网络传播的，但他们对此却无能为力。索恩伯里起草的法规将规定，阻断恐怖分子通过网络联系和计划恐怖袭击的网络袭击是“传统”军事行动。

2011 年 06 月 02 日 网易新闻
http://war.163.com/11/0602/09/75HLAMJP00011MTO.html