網路攻擊、網路間諜及網路監控之國際法評價

魏 靜 芬*

目 次

壹、前言
貳、網路攻擊與武力攻擊
一、「武力行使」的概念
二、「武力行使」的態樣
三、「武力威脅」的意義
四、武力攻擊
五、網路攻擊
參、網路攻擊之國際規制
一、國際不法網路行為之國家責任
二、網路間諜
肆、和平時期網路監控活動的評價
伍、結論

* 國防大學管理學院法律學系暨研究所教授。國防部國際法律事務研究諮詢會委員、國防部法規會委員、臺灣海洋事務策進會理事長。日本九州大學法學博士。

壹、前　言

現代科技的進步造成現今社會日益依賴電腦與網路完成各項工作，除了增進作業的便利性外，另外卻也存在更多的網路安全問題，諸如電腦病毒、駭客侵入及盜竊機密資料等。電腦病毒在網路上的流竄，除企業與軍事單位外，重要的國家建設如電力設施、通訊網路、金融體系與交通設施同樣容易成為攻擊目標，一旦遭受網路攻擊，即可能引發社會動亂，進而癱瘓整個國家運作。

隨著戰爭手段的改變，近年來國際間發生網路攻擊。所謂網路攻擊係指攻擊者透過網際網路對被攻擊之電腦裝備、資訊系統及資訊流運作等，實施阻絕、衰退、擾亂、竊取、詐欺、竄改、摧毀等行為[1]。網路攻擊可藉由電腦病毒侵入各種網路應用領域，並得滲入各機關或組織內部電腦進行攻擊、癱瘓或破壞等，甚至造成實體上損害，較傳統攻擊手段更具靈活性及多樣性；網路攻擊所耗費的成本，遠低於傳統攻擊費用，而所造成的人員傷亡與設施破壞，相較於傳統的軍事攻擊幾乎具有同等的嚴重程度[2]。國際間多數國家均認為未來網路戰爭將不再是屈居不對稱戰力的附屬地位，因此紛紛成立獨立的資訊軍種部隊及相關的指揮結構體系。

近年來國際實踐中不乏有網路攻擊的案例發生。2007 年愛沙尼亞因移動第二次世界大戰的蘇軍紀念碑，引起俄羅斯的強烈不滿，愛沙尼亞遭受來自俄羅斯的網路攻擊，其總統府、議會、政府各部門、主要政黨、媒體、銀行和各大公司的網站幾乎全數癱瘓達數週之久[3]。再者，2008 年 8 月，喬治亞共和國與俄羅斯的軍事衝突，在雙方軍隊未交戰前，俄羅斯的網路戰部隊即對喬治亞共和國展開全面網路攻擊，致使喬治亞共和國政府與民間網站幾乎處於癱瘓或關閉狀態；而在宣布停火後，雙方網路攻防仍持續進行激烈對抗[4]。換言之，各國間的軍事攻擊已不僅侷限在傳統的武力攻擊，亦逐漸延伸至網路上的互相較勁。至於網路攻擊是否可視為聯合國憲章第 51 條所定的武力攻擊行為？其法律定位如何，國際間如何規制，皆是值得探討與釐清之議題。再者，網路空間上的監控活動，在和平時期的監控，是否對他國構成主權侵害；以及在符合一定條件下是否有可能構成國際法上的間諜行為，本文擬從國際法上的評價來逐一分析、探討。

1　梁華傑，〈網路戰資訊安全探討與省思〉，《國防雜誌》，2008 年 6 月，第 23 卷第 2 期，頁 109。

2　網路攻擊的方式計有竊取機密資料、癱瘓資訊系統、侵入電腦控制系統藉以摧毀資訊或支持資訊的基礎設施，諸如發電廠、供水系統、水庫、電訊、交通、廣播電視、航空航海等；達到實際使軍事設備、武器損壞或暫時失靈或產生錯誤功能；造成人員直接或間接傷亡。

3　今日新聞網，〈http://www.nownews.com/2007/05/17/91-2098046.htm〉，最後瀏覽日：2011 年 12 月 8 日。

4　中華民國國防部網站，〈http://www.mnd.gov.tw/Publish.aspx?cnid=65&p=28600〉，最後瀏覽日：2011 年 12 月 8 日。