中共、台灣資安問題

**要講台灣在資安國防的隱憂與問題，必先提到中國在設立”網軍”的歷史與目的。**

1986 年受波灣戰爭影響，著手組建數位化部隊，研究新型態的資訊作戰方法。

1995 年和 1996 年成立「國防科技信息中心」、「信息安全研究室」及於「總參二部(軍事情報部)」下成立「科學裝備局」等機構，進行研發資訊軟硬體、電腦病毒、駭客攻擊、電磁脈衝武器等技術，作為先導研究。

1999 年 11 月解放軍報首次提出「網軍」，成為繼陸、海、空三軍 及二砲後的新「軍種」軍分為攻擊、防衛、維護三大部門。

其目的主要在藉由網路的漏洞，竊取公家甚至民間的機密資料，甚至竄改資料、癱瘓系統

「武器」則分別使用「間諜程式」、「蠕蟲程式」、「木 馬程式」、「釣魚程式」及「電腦病毒」等，透過網路入侵各國政、軍、 經電腦系統。

**真實案例:**

1. 德國資訊安全局（BSI）調查發現，中共積極培養「電腦間諜（Computer-Espionage）」，全方位對德國聯邦政府各部門蒐集戰略機密資訊，獲取德國高科技產業的機密資訊，以提昇中共軍工科技研發能力。由此顯見，中共的資訊戰能力，已讓科技立國的德國頭痛不已
2. 中國的天網系統監控系統無所不在，現已有1.7億個監控鏡頭遍布各地，當局計畫未來3年要再安裝4億個。只要被天網鏡頭鎖定，馬上就可以分析出他的年齡、種族、性別、衣著、表情。英國BBC記者親測，只「潛逃」7分鐘就被公安抓到。天網的存在一直被質疑侵犯人權和隱私，雖然官方表示，只有必要的時候才會用到。不過如果被黑帽駭客利用，將會是一場前所未有的大災難。
3. 有位學者出身的政務官在被宣布延攬入閣當天，其秘書就接到一封惡意郵件，這封郵件假藉秘書名義寄給各部會，一打開就中毒，被植入惡意程式，駭客可藉此入侵中華民國政府機構的內部網路。

**防治方法**

科技始終來自於人性，資安的關鍵不在技術，而在「人安」，依照美國資安研究單位的測試發現，假訊息、郵件的滲透可以達到人際關係的第八層， 滲透率極為驚人。同時，點閱不明來信者的人，將近　20%　相信他們自 己認識發信者或信賴瀏覽器，可見人性才是資安的最大弱點。