從戰爭的觀點論資訊安全

資訊安全之所以會成為問題，乃是有人蓄意破壞。
打贏這個敵人，才有安全可言。
打贏，是一種藝術。

台大資訊工程系　湯耀中 教授　編著

全華科技圖書股份有限公司 印行

從戰爭的觀點論資訊安全

湯耀中教授　編著

全華科技圖書股份有限公司　印行

序

本書係依據作者在台大資訊工程研究所講授課程「網路資訊安全」內容整理而成。適用於類似課程之參考教材，或企業政府部門資訊管理人員的參考資料。

本書之一主要特點，是從戰爭的觀點，切入探討資訊安全的本質及相關題目，亦即把資訊安全，視作進行一場戰爭，打贏了，才有安全。和許多市面上的期刊，雜誌，書籍，把資訊安全和防火牆，入侵偵測，公鑰基礎建設，防毒軟體等，劃上等號，有很大的不同。戰爭，當然要有明確的戰略思維及戰術運用。人類從事資訊安全的研究，不過十來年的歷史，對於戰爭，卻有累積數千年之經驗。本書探討問題的一個重要方法，即是從人類的戰爭經驗裡，透過類比的邏輯思維，嘗試在戰略戰術層次，為資訊安全找出一些指導原則。中國古代大戰爭思想家孫武的理論，許多亦可用於資訊安全領域內。從戰爭的角度看資訊安全，我們得到許多具顛覆性的戰略戰術指導原則，例如安全是沒有標準的，認證只是強權資訊攻擊的一種策略，所謂公正的第三者是不可能的，政府公權力對資訊安全的正面作用有限，隱私資訊是資訊安全的制高點，因敵制勝與將能君不御為致勝的關鍵等。

攻勢戰法和守勢戰法，是資訊攻防所可運用的工具，好比是一塊電路板上之電阻，電容，晶片等元件。將各種元件，適當的搭配組合，形成一個可運作的電路板。組合的技巧，可視之為戰術。要組合出幹什麼用的電路板，可謂之戰略。顯然地，有高明的戰略，戰術，豐富的工具資源，才可做出賣錢的好電路板。是以本書對於現在已知各種資訊攻防戰法，做一介紹。以易經為基礎之三十六計，亦可用為資訊戰術之指導原則。

目前許多企業的資訊部門的高階主管，或政府資訊部門的高層人士，在學校唸書的時候，恐怕根本沒有聽說過網路資訊安全這個名辭，當然也沒有修過類似的課程。他們對這個問題的認知，多半來自於職場的實務經驗，或者是來自各種安全設備的提供者，或者來自於各種商業電子期刊的報導文章，或者是參考各種短期訓練課程。所得的資訊，往往是支支片片，卻少從頭到尾的一貫性。在不知不覺中，會被〝用了某家公司的防火牆，就會比較安全，〞或〝某個牌子的入侵偵測系統，功能較多，比較安全，〞等不正確的念頭牽著走而不自覺。

作者撰寫本書，儘量嘗試用一般的語言，少用專業術語，希望不具電腦專業的人士，亦無閱讀上的困難。閱讀本書之後，希望讀者能建立起自己的思維，當碰到一個新的環境，能夠自己思考，自己研判，如何做，才會是安全的，或者，如何做，才不安全。能夠自己思維判斷，往往可以花少許的經費，就達到安全的效果，反之，會花上大筆的經費，卻依然不安全。

過去幾年，選修作者「網路資訊安全」課程的同學，都會繳交學期報告。其中不少同學的報告，剖析問題十分清楚。對本書撰寫，有所助益。不克一一列舉，利用此機會，謝謝他們。

當然，沒有家人的包容協助，及台大資訊工程系給予開課的機會，這本書，是不可能寫出來的，一併致謝。

作者　湯耀中

目錄

1 · 序言

1-1 資訊戰爭 1-2
1-2 政策、大戰略、戰略 1-4
1-3 結合歷史、科技與哲學的藝術 1-6
1-4 主事者的戒律 1-8

2 · 不可

2-1 不可相信安全標準 2-2
2-2 不可迷信認證 2-15
2-3 不可依賴法律條文或檢調機構 2-22
2-4 不可信賴所謂公正第三者 2-34
2-5 不可輕忽個人隱私資訊是資訊安全制高點的道理 2-46
2-6 不可遺忘資訊安全是相對的之基本道理 2-63

3 · 以古為鏡

4 · 攻勢戰法

4-1 電腦蒐集分析資訊 4-2
4-2 形象塑造與心理戰 4-5
4-3 內賊 4-12
4-4 信息竊聽 4-21
4-5 入侵電腦 4-35
4-6 偽裝 4-49
4-7 網路傳染病 4-62

5 · 守勢戰法

5-1 亂與隱 5-2
5-2 辨識真偽 5-29
5-3 監控 5-49

6 · 以卅六計為戰術

6-1 勝戰計 6-3
6-2 敵戰計 6-23
6-3 攻戰計 6-45
6-4 混戰計 6-60
6-5 併戰計 6-75
6-6 敗戰計 6-95

CHAPTER 1

序 言

資訊安全之所以會成為問題，乃是因為有敵人存在，敵人無時無刻不思入侵之道。所以要求資訊安全，就是要打敗這個敵人。

1.1 資訊戰爭

桃樂絲丹寧(Dorothy E. Denning)為喬治城大學研究資訊戰爭(Information Warfare)的名教授，在其所著資訊戰爭與安全(Information Warfare and Security)一書中，為廣義的資訊戰爭下定義為「資訊戰爭的攻擊，其目的是使資訊資源對於入侵者的使用價值增加或對於防禦者的使用價值的減少。」美國國防大學資訊戰爭及戰略學院院長約翰愛爾格(John Alger)認為「資訊戰爭作戰行動的特質，是保護、壓榨、腐化、拒絕或摧毀資訊或資訊資源，以便擊倒對手或從對手得到好處。」

資訊資源，依功能可區分為五類，即媒體、載具、感測器、記錄器及處理器。媒體是指磁帶、磁片、電腦記憶體、人腦記憶體、紙張等，媒體可以儲存資訊，本身可能有一定的結構。載具是指通訊設備，可將資訊一地傳送至另一地。感測器如人之五官，攝影機、麥克風、掃瞄器等，可以從周遭環境，或者某一個物體上，抽取出資訊。記錄器可把資訊放入載具，如磁碟機、印表機等。處理器可以處理資訊，如人之大腦，微處理器，電腦之硬軟體等。一組資訊資源組合起來，就構成一個資訊系統，在這個系統裡面，資訊可以流傳來，流傳去。

駭客竊取到某個資訊系統的某個使用者的密碼之後，就可以使用該資訊系統，對於這個駭客而言，該系統的使用性增加了。依照桃樂絲丹寧的定義，這種行為是一種資訊戰爭的作戰行動；於網路上散佈病毒，使中毒電腦的硬碟機上的資料全部毀掉，中毒電腦的擁有者，對於它的使用性，減少了，所以，放置病毒是一種資訊戰爭的作戰行為。

資訊安全(Information Security)一詞，已經有卅餘年的歷史。美國聯邦政府的安全準則，將資訊安全定義為「保護資訊，使之免於遭受故意或無意的洩露、移轉、變更、毀壞」所謂無意的，是指例如因停電、地震、失火等非人為的因素，使得資訊外洩或損害。所謂故意的，就是指

防禦性的資訊戰爭，也就是指破壞的源頭，是源於人為的設計，必須至少有一個這樣的敵人，才會造成資訊不安全。防禦性的資訊戰爭，亦有人稱之為資訊保全(Information Assurance)。本書內資訊安全一語等同資訊保全。

桃樂絲丹寧資訊戰爭的定義，是一種廣義的定義，因為參與資訊戰爭的，並不僅限於傳統戰爭的的軍事單位，也不僅限於國家與國家的衝突。資訊戰爭的參與者，依其本身之能力及可支配的資訊資源，可以概括地區分為三類，即個人、公司及國家；個人是指參與者是某一個人或某一小組人，所能支配的僅是幾部個人電腦，常常見報的駭客，即是屬於此一類型；公司是指參與者是一組人，具有一定的組織及財務能力，其所能支配的資訊系統往往是很多個電腦所構成的一個網路，銀行，就是一個典型，公司型態的資訊戰爭的參與者，但也很不幸，往往是被攻擊的一方，世界性的恐怖組織，是另一種公司型態的參與者，而且是攻擊性的；國家型態的參與者，包括了一個國家的軍事單位、情治單位、國安單位、各級政府機構，其所擁有的人力資源、財力資源，可以視之為「無限大。」1999 年台灣政府提出兩國論的說法時，台灣政府機構，遭受到七千多次來自中國大陸駭客的攻擊，是一種「國家與個人」的資訊戰爭。為方便計，將用＜國家，個人＞，代表個人型態的參與者，攻擊國家型態的參與者，用＜公司，公司＞代表公司型態的參與者攻擊公司型態的參與者。餘類推，共計有九種可能的不同組合，每一組合，可以視為是一種資訊戰爭的型態。下面列舉此九種型態，及可能的實例。

- ＜國家，國家＞ 國防與國家安全。
- ＜國家，公司＞ 國際恐怖組織活動。
- ＜國家，個人＞ 駭客攻擊政府機構。
- ＜公司，國家＞ 國家安全，打擊犯罪。
- ＜公司，公司＞ 商業間諜。
- ＜公司，個人＞ 竊取公司機密資料以得利。
- ＜個人，國家＞ 利用個人隱私，以打擊異己、打擊犯罪。
- ＜個人，公司＞ 利用個人穩私資料行銷。
- ＜個人，個人＞ 電腦犯罪。

1.2 政策、大戰略、戰略

戰爭是自有人類以來，就存在的，人類歷史中，產生不少戰略思想家，教導相信他的人，如何打贏敵人，西方世界裡，十八世紀末，十九世紀初的拿破崙，是公認的一位卓越軍事家(1769～1821)。較拿破崙稍晚的普魯士人克勞塞維茲(Carl Von Clausewise，1780～1831)著戰爭論一書，是西方戰爭理論的經典。廿世紀，西方戰爭思想的代表人物，當推富勒、李德哈特與薄富爾。富勒(J. F. C. Fuller)是英國人，接受正規的軍事訓練，1917 年康布萊戰車會戰計畫便是出自其手，1963 年獲得英國三軍學會的最高榮譽獎章，著有戰爭指導(The Conduct of War 1789～1961)，及西洋世界軍事史。李德哈特(1895～1970)是英國軍事思想家，其關於機械化戰爭的觀念，對於當代的戰爭藝術具有重大的影響，著有戰略論等卅餘冊著作。薄富爾(Ander Beaufre)，法國將軍及戰略思想家，1902 年生，1975 年逝，享年 73 歲。曾任北大西洋公約組織常設小組法國代表，官拜上將。1961 年退役，致力於戰略思想著作，陸續推出「戰略緒論」、「嚇阻與戰略」、「行動戰略」及「明日戰略」等書。

東方戰爭思想家，捨孫武其誰。孫武，字長卿，生卒年代大約和孔子(551BC～479BC)同時，所著「孫子兵法」一書，是世界現存的最早的兵書，歷來被視為「兵經」，為古今中外，軍事家所尊崇，曾培育了我國歷史上如戰國的孫臏、慰繚，漢代的韓信，唐代的李靖，宋朝的岳飛等等眾多的著名將領。孫子兵法問世後，對古代軍事學術的發展產生了巨大而深遠的影響，歷代兵學家，軍事家無不從中汲取資料。「諸觀兵書，無出孫武」，「前孫子者孫子不遺，後孫子者不能遺孫子」，這乃是人們對孫子地位和「孫子兵法」一書價值的普遍認同。「孫子兵法」本共十三篇，六千餘字，前六篇：計篇、作戰篇、謀攻篇、形篇、勢篇、虛實篇，是孫武教導人們如何打敗對手的基本指導原則。

李德哈特於其戰略論第十九章，對於戰略擬定簡短的定義，「戰略是分配和運用軍事工具，以來達到政策目的的藝術」，當軍事工具的運用，最後終於和實際戰鬥合為一的時候，此時如何控制和處理那些直接行動的方法，遂被稱作是「戰術」。戰術是把戰略運用到較低的一個層次。大戰略就是協調和指導一個國家的一切力量，使其達到戰爭的政治目的，它所涉及的層面，不僅是軍事而矣，當要顧及到經濟面、人力面、精神面等。大戰略所看到的，不僅贏得戰爭，還要看到，贏得戰爭後和平的狀況。政策是一個國家的方向，政策決定一個戰爭的政治目的。

資訊戰爭，是一種戰爭的型態，軍事思想家提出教導信仰者如何打贏戰爭的指導原則，亦可用於資訊戰爭，資訊保全，亦當然適用。此也就是說，軍事思想家的智慧結晶，提供一條明確的路線，落實資訊保全。

1.3 結合歷史、科技與哲學的藝術

網路安全之所以成為問題，是因為有人蓄意的破壞，也就是說，是因為有「敵人」的存在。網路安全，其實就是和「敵人」的對抗，本質上，是一種戰爭。戰爭，是一結合歷史，科技與哲學的藝術。人類從事於戰爭的研究，已經有數千年的歷史，累積了許多的智慧的結晶，指導人們如何獲取一場戰爭的勝利。

資訊保全，就是要將古往今來，軍事家提出來的戰勝敵人的指導原則，靈活的運用到資訊安全領域，並藉之發展出各種確保資訊安全的策略、手段與工具。軍事家告訴我們，只有防禦，是打不贏戰爭的，因此，在我們的概念中，資訊安全，不能僅有防禦，更要有攻擊的力量。

研究歷史，是因為瞭解到資訊安全相關的問題，是無法以類似工程的方式，從小型的模式，推導出大型系統的結果，或者說，無法在實驗室內實驗的，因此，必須從歷史事件中汲取教訓，即「以古為鏡，可以知興替。」以往戰爭的歷史，各種資訊安全事件的報導，資訊安全相關攻擊防禦工具的發展過程等，均是探討的範圍。將已知工具的特質，分類量化，亦是一重點工作。

哲學，指的是思維，平日，對於敵我雙方能力的評估，要落實精確，在思想領域內，對於敵人將來可能的動作，要預先設想，並求破解。敵我對抗、戰略、戰術、戰法的發展與製定，都必須在思想領域內，有一個明確的認知與辯證，才能在一旦有真正衝突時，派上用場。從事哲學方面的探討，將涵蓋資訊安全方面之國家政策，大戰略、戰略、戰術、戰法各層次。

科技，指的是資訊安全的各種工具。戰略，根據廿世紀大戰略家李特哈德的說法，是支配與運用各種戰爭(資訊安全)工具的藝術。戰術，其實就是小規模的戰略。掌握不了工具，想打贏戰爭，是幾乎不可能的。工具，可概括分為防禦與攻擊二大類，均是近代科技的運用。從歷史、哲學中，會提示我們新的工具應有的特質，再運用科技，將之實現。

1.4 主事者的戒律

拿破崙的戰爭哲學是〝將道〞，他認為在戰場上，一個將領的智慧與判斷，才是勝利的關鍵。孫子兵法計篇，把道、天、地、〝將〞、法列為決定戰爭勝負的五個基本因素。〝將孰有能〞為一關鍵，和拿破崙的思想一致。〝將者、智、信、仁、勇、嚴也。〞智，指的是智謀才能，指的是智慧，就是要有思想。在資訊安全的領域裡，兵書裡所謂的〝將〞，就相當於各企業機構裡的資訊室主任或安全室主任或電子商務部主管。或概稱之為主事者。主事者的智謀才華，對於一個資訊系統的安危，有著決定性的影響。主事者的思維，當然不能是憑空亂想，而是要有一定的指導原則。從過去的經驗裡，整理出六個主事者的戒律，以為主事者思維或訂定安全計畫的思想依據或指導原則。

主事者的戒律是：

一、不可相信安全標準，以為嚴格遵行標準就會安全。

二、不可迷信認證，以為經過認證的產品或系統就一定安全。

三、不可依賴法律條文或檢調機構，以為其對資訊安全有正面幫助。

四、不可信賴所謂公正第三者。

五、不可輕忽個人隱私資訊是資訊安全制高點的道理。

六、不可遺忘資訊安全是相對的之基本道理，要隨時落實評估可能敵人實力。

資訊安全之所以會成問題，根本原因是有人蓄意破壞。破壞者，哪裡會遵守「標準方式」從事破壞。防禦者，死守某個標準，不等於教人如何打你，是很不智的。既然沒有安全標準，又從何認證呢？更何況認證制度：如 FIPS140，是資訊強權用以瓦解相對弱國資訊防禦的策略。資訊安全的本質，是和入侵者進行一場資訊戰爭，講求的是「出奇制勝」，主事者依標準辦事，崇拜認證制度，是求敗。在資訊系統裡，沒有自然力留下的證據，亦沒有不在場證明，想靠司法力量，事後抓到壞人，給予制裁，以收嚇阻之效，顯然不會有效。事前周全的措施，讓壞事發生的可能率降至極低，才是正確主事者心態。

當今很多資訊系統安全機制的設計，都假設有一個公正的第三者存在：如憑證機構。在真實社會裡，法院是可接受的公正第三者，但別忘了，其公正性的前提是「不告不理」，法院扮演著被動角色。資訊安全裡的公正第三者，卻是主動地「事事參與」，和法院完全相反，甚至要靠賣「公正」來賺錢，倒像是「法老王的祭師」，利用一般大眾對資訊安全知識不足的弱點，幫特定對象聚財，「公正」只是一種裝飾。主事者盲從公正第三者，後果可想而知。

「依照政府規定的去做，就不會錯」，是不少資訊主管的心態。對攻擊者而言，「勝可知，不可為」，防禦者自露敗相，是攻擊成功的主因。每一個資訊系統，其主觀環境，可能敵人能動用的資源，皆不相同，政府哪會完全知道。照政府規定，一定是顧東忘西，不周全，而給敵人有機可趁。

安全，有一種有趣的現象，即什麼都不做，也未必會出事。此就給系統內工作人員很大的空間，可以把有限的資源，去做一些和安全無干的事，而未必倒楣出事，也就是說，以安全做幌子，A 錢很容易。「內賊」是資訊事故很主要的因素。據統計，有百分之七十的事件和內賊有關。取得員工的隱私資料，攻擊者才能設法誘使員工叛變。另外，隱私資料是猜測密碼的有效線索。

黑盒子式的硬體設備，是木馬或後門程式的良好棲息地。對不肖的安全設備製造商而言，販售一萬個正常設備的利潤，可能抵不上一個有後門的。誘因太大。用「白盒子」，即內部構造透明，使用者能充分了解者，才不會有問題。安全，既然是一種戰爭，當然是相對的，是敵我互動的，是要時時評估對手，才有致勝機會。

「我不告訴你我怎麼做，你就攻擊不了我」。聽似有理，其實不對。合理做一件事的方法往往有軌跡可循，要猜出來不難。靠保密，求安全，是要保護密碼，通常是一個亂數，只有自己知道。

刑事局曾經發佈資料隱碼攻擊法警訊，號稱全台有八成網站擋不住。新聞對於該攻擊法說明並不清楚，其因應之道，竟然是去找某家網路安全公司。但從 GOOGLE 網站上，可查到的相關網頁有三千六百張，此為一討論甚久的攻擊法，和其它成千上萬種攻擊法比較起來，並未有特別突出之處。這種攻擊法，只要在資料輸入時，不准有單引號「'」即可避免，防禦相當容易。用此法攻擊，要有破壞力，不僅得原程式撰寫人很不小心，而且要有系統管理者之權限，很不容易。在 GOOGLE 搜尋器裡，找不到一個實例。如是，令人懷疑，不知是「安全警訊」還是「安全廣告」。不過，倒為戒律三提供一佐證。

在一個資訊系統裡，消費者或末端使用者，是在系統的建置或設計的過程中，沒有參與，只能照著系統規定的去做的人。例如在網路銀行裡，客戶就是末端使用者，客戶只能依照網路銀行的規矩去做。所以，從客戶的角度來看，客戶的唯一選擇權，就是找一家他認為比較安全的銀行往來，而避開他認為不安全的銀行。但是，消費者又如何判知哪家銀行比較安全呢？消費者又不是電腦專家，也不是資訊安全專家，怎麼會有這方面的能力呢。本章論及的六誡，提供消費者或一般大眾一個指南，可以憑著每個人自己的主觀認知，去判斷或去打聽，所要往來的銀行，其經營型態狀況，有沒有違反六誡。若消費者主觀上覺得有，就不要和這家銀行往來。這裡提到的主觀，是說不用去嚴謹的蒐集科學上的證據或法律上的判決，只要消費者覺得有就可以了。比如說，問過幾個親朋好友，都說這家銀行違反第一條，就可主觀上認定，不必去請個徵信社，花大量精力去調查個水落石出。

CHAPTER 2

不　可

吳子兵法：「故將之所慎者五：一曰理、二曰備、三曰集、四曰戒、五曰約。」「戒者，雖克如始戰。」

本章所論者，乃資訊戰爭將領之戒，亦即要隨時戒慎恐懼，不要犯不該犯的錯誤。